TRABAJO FIN DE GRADO.

Grado en Derecho.

Facultad de Derecho.

Universidad de La Laguna.

Curso: 2022/2023.

Convocatoria: Julio.

PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS: ANÁLISIS DE LA LEGISLACIÓN EUROPEA Y ESPAÑOLA EN EL CONTEXTO DE LA IMPLEMENTACIÓN DE INTELIGENCIA ARTIFICIAL (IA).

DATA PROTECTION IN PUBLIC ADMINISTRATION: ANALYSIS OF EUROPEAN AND SPANISH LEGISLATION IN THE CONTEXT OF THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE (AI).

Realizado por la alumna: Dª. Melanie Catherine Coello Ramos.

Tutorizado por el Profesor: D. Ángel Lobo Rodrigo.

Departamento: Disciplinas Jurídicas Básicas.

Área de conocimiento: Derecho Administrativo.

ABSTRACT

Currently, data protection and artificial intelligence are relevant topics in public administration. Digitization and the use of advanced technology pose challenges in terms of privacy and handling sensitive information.

The European Regulation (GDPR) establishes principles and obligations to ensure the protection of personal data. In Spain, the Organic Law 3/2018, 5th of december, Personal Data Protection & Digital Rights Guarantee (LOPDGDD) complements and develops the GDPR, adapting it to the national context.

Artificial intelligence has the potential to improve efficiency and service quality but raises ethical and legal challenges. A Law on Artificial Intelligence has been proposed in Spain to regulate its use, especially when it comes to the public sector.

It is crucial to consider data protection aspects when applying artificial intelligence in the public sector. This includes ensuring the privacy and security of data, promoting transparency, addressing bias and discrimination, and establishing applicability mechanisms in decisions made by Artificial Intelligence systems.

Key Words: Data protection, artificial intelligence, public administration, GDPR, LOPDGDD, privacy, digitalization.

RESUMEN

En la actualidad, la protección de datos y la inteligencia artificial son cuestiones relevantes en las administraciones públicas. La digitalización y el uso de tecnologías avanzadas plantean desafíos en cuanto a la privacidad y el manejo de información sensible.

El Reglamento General de Protección de Datos establece principios y obligaciones para garantizar la protección de los datos personales. En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) complementa y desarrolla el Reglamento, adaptándolo al contexto nacional.

La inteligencia artificial tiene potencial para mejorar la eficiencia y calidad de los servicios pero plantea desafíos éticos y legales. Se ha propuesto una Ley de Inteligencia Artificial para regular su uso, especialmente en el ámbito público.

Es crucial considerar aspectos de protección de datos al aplicar la inteligencia artificial en el sector público. Esto incluye garantizar la privacidad y seguridad de los datos, promover la transparencia, abordar el sesgo y la discriminación, y establecer mecanismos de aplicabilidad en las decisiones tomadas por sistemas de IA.

Palabras Clave: Protección de datos, inteligencia artificial, administración pública, RGPD, LOPDGDD, privacidad, digitalización.

ÍNDICE

1. INTRODUCCIÓN.

En la era digital, las Administraciones Públicas se encuentran inmersas en un proceso de transformación y modernización que busca mejorar la eficiencia y la calidad de los servicios ofrecidos a los ciudadanos. En un primer momento, se ha podido observar en el Trabajo de Fin de Grado de mi compañero Miguel Ángel Labrador Orellana, que la Unión Europea y, en concreto, España, ha estado inmersa en el desarrollo de la digitalización dentro de las Administraciones Públicas como el caso de la Sede Electrónica, el PIN Permanente, la Clave Digital, el Registro Electrónico, etc[1]. En este contexto, la implementación de la inteligencia artificial (en adelante, IA) ha ganado terreno como una herramienta prometedora para automatizar tareas, optimizar procesos y tomar decisiones basadas en datos. Sin embargo, esta adopción masiva de la IA también plantea desafíos significativos en términos de protección de datos y privacidad.

La protección de datos personales se ha convertido en una preocupación real en el ámbito de las Administraciones Públicas, ya que manejan grandes volúmenes de información sensible de los ciudadanos. La implementación de la IA introduce nuevos riesgos y vulnerabilidades, ya que implica la regulación, el análisis y el uso de datos personales en una escala sin precedentes. El tratamiento inadecuado de estos datos podría conducir a violaciones de la privacidad, discriminaciones aleatorias y pérdida de confianza por parte de los ciudadanos.[2]

El objetivo de este Trabajo de Fin de Grado es analizar en profundidad los desafíos y las implicaciones de la protección de datos en las Administraciones Públicas en el contexto de la implementación de la inteligencia artificial. La indagación se centrará en comprender cómo la IA afecta a los ciudadanos y cómo se puede garantizar una protección efectiva de los datos personales en este entorno tecnológico en constante evolución.

---

[1] LABRADOR ORELLANA, M.A. (2023). Trabajo Fin de Grado *"La Sede Electrónica en la Administración General del Estado (A.G.E): Identificación, Registro, Notificación y Verificación de Documentos"*. Pág. 39. (fecha de última consulta: 12-07-2023).

[2] ZUBOFF, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs. pág. 287 (fecha de última consulta: 12-07-2023).

Por tanto, se analizará el marco legal y normativo existente en relación con la protección de datos en las Administraciones Públicas, prestando atención a las implicaciones que tiene la IA en aspectos como la identificación, en primer lugar, de la normativa aplicable en el entorno europeo y, específicamente, en la legislación española alrededor de la protección de datos; así como la identificación de los métodos de utilización de la inteligencia artificial en las Administraciones Públicas y su actual o futura regulación. Posteriormente, se identificarán estos factores y se analizará, finalmente, la intersección entre la protección de datos y la inteligencia artificial en el sector público.

Para llevarlo a cabo, se utilizará una metodología que combina una revisión bibliográfica exhaustiva de las regulaciones, normativas y estudios relevantes en el ámbito de la protección de datos y la IA en el sector público.

Por consiguiente, se espera contribuir al conocimiento existente sobre la protección de datos en las Administraciones Públicas y proporcionar las recomendaciones prácticas para garantizar una implementación responsable de la IA que respete la privacidad y derechos de los ciudadanos.[3] Además, se impulsa la creación de conciencia sobre la materia en cuestión, promoviendo así la confianza de los ciudadanos, fomentando una actuación administrativa desde una perspectiva ético-social.

Asimismo, se realiza una aportación de conocimientos significativos y prácticos, además de generar una reflexión más amplia sobre el equilibrio necesario entre la implementación de la inteligencia artificial y la garantía de protección de los derechos fundamentales de los ciudadanos en las Administraciones Públicas.

En los siguientes capítulos, se explorarán con mayor detalle todos estos aspectos.

[3] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (AEPD). (2021). Guía de Protección de Datos y Privacidad en las Administraciones Locales. Disponible en: https://www.aepd.es/media/guias/guiaprivacidadentidadeslocales.pdf

(fecha de última consulta: 12-07-2023).

2. PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS.

2.1 Introducción.

En esta sección se examinará la legislación y las regulaciones que se aplican específicamente a la protección de datos en el ámbito de las Administraciones Públicas, tanto a nivel europeo como estatal. Esto se realiza para asegurar la privacidad y la seguridad de los datos personales que son gestionados por las instituciones gubernamentales.

2.1.1 Legislación europea aplicable a las Administraciones Públicas.

Se examina el marco legal europeo relacionado con la protección de datos y su aplicación en las Administraciones Públicas. En particular, se destaca el Reglamento General de Protección de Datos (RGPD),[4] que establece normas y principios para el tratamiento de datos personales en toda la Unión Europea. Se analizan los aspectos claves del RGPD que son relevantes para las Administraciones Públicas, incluyendo:

En primer lugar, los principios fundamentales de protección de datos[5]:

- **Principio de licitud, lealtad y transparencia:** Los datos personales deben ser tratados de manera legal, justa y transparente, con el consentimiento del titular de los datos cuando sea necesario.

- **Minimización de datos:** Se debe recolectar y retener la cantidad mínima de datos personales necesarios para cumplir con los propósitos específicos del tratamiento.

[4] GARCÍA-CAPELO, A.,& GARCÍA,S. (2019). La protección de datos en las Administraciones Públicas: Un análisis a la luz del Reglamento General de Protección de Datos (RGPD). Ediciones Cívitas. (fecha de última consulta: 12-07-2023).

[5] GUICHOT, EMILIO. (2005). Datos personales y Administración Pública. Madrid: APDCM-Thomson-Civitas. Pág. 230-234. (fecha de última consulta: 12-07-2023).

- **Exactitud:** Los datos personales deben ser precisos y actualizados, y se deben tomar medidas para corregir o eliminar cualquier información incorrecta o desactualizada.

- **Limitación de la finalidad:** Los datos personales deben ser recopilados con fines específicos y legítimos, y no deben ser procesados de manera incompatible con esos fines.

- **Conservación de los datos:** Los datos personales deben ser mantenidos en una forma que permita la identificación de los sujetos de datos solo durante el tiempo necesario para cumplir con los propósitos del tratamiento.

En segundo lugar, las obligaciones y responsabilidades de los responsables del tratamiento de datos[6]:

- **Seguridad de los datos:** Los responsables del tratamiento, incluyendo las Administraciones Públicas, deben implementar medidas técnicas y organizativas apropiadas para proteger los datos personales contra el acceso no autorizado, la divulgación, la alteración o la destrucción.

- **Notificación de violaciones de datos:** En caso de que ocurra una violación de seguridad que pueda comprometer los derechos y libertades de los individuos, los responsables del tratamiento deben notificar dicha violación a la autoridad de protección de datos competente y, en ciertos casos, también a los individuos afectados.

- **Designación de un Delegado de Protección de Datos (DPD):** Las Administraciones Públicas, en calidad de responsables del tratamiento, pueden estar obligadas a designar un DPD que sea responsable de supervisar y asesorar sobre cuestiones relacionadas con la protección de datos.

---

[6] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (AEPD) (2020).Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento. Disponible en: https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf

(fecha de última consulta: 12-07-2023).

En tercer lugar, las transferencias internacionales de datos y mecanismos de adecuación[7]:

- **Transferencias internacionales de datos:** Cuando se transfieren datos personales fuera de la Unión Europea, existen requisitos específicos para garantizar que los datos estén protegidos de manera adecuada en el país receptor.

- **Mecanismos de adecuación:** Los mecanismos de adecuación son medidas adoptadas para asegurar que las transferencias de datos a países fuera de la UE se realicen de acuerdo con el nivel de protección requerido por la legislación de protección de datos de la UE. Ejemplos de estos mecanismos incluyen las cláusulas contractuales tipo y el Escudo de Privacidad *(Privacy Shield)*.

El RGPD establece un marco legal para la protección de datos personales en toda la Unión Europea como se expresó anteriormente. Algunos artículos clave del RGPD que son especialmente relevantes para las Administraciones Públicas son los siguientes:

- **Artículo 5:** Este artículo enumera los principios fundamentales que las Administraciones Públicas deben cumplir en el tratamiento de datos personales. Estos principios incluyen la licitud, lealtad y transparencia en el tratamiento de datos, la minimización de datos, la exactitud de la información, la limitación de la finalidad y la conservación de los datos analizados previamente.[8]

---

[7] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) (2020).Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento, pág 28. Disponible en: https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf (fecha de última consulta: 12-07-2023).

[8] 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 (en adelante, Reglamento General de Protección de Datos), pág 35. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf (fecha de última consulta: 12-07-2023).

- **Artículo 6:** Este artículo establece las bases legales que justifican el tratamiento de datos personales por parte de las Administraciones Públicas. Algunas de las bases legales relevantes incluyen el cumplimiento de una obligación legal, previsto en el apartado *c),* que establece *"el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"*, el cumplimiento de una misión de interés público o el ejercicio de poderes públicos conferidos a la institución. [9]

- **Artículo 9:** Este artículo se refiere al tratamiento de categorías especiales de datos personales, como aquellos que revelan origen étnico, opiniones políticas, creencias religiosas, afiliación sindical, datos genéticos o biométricos, entre otros.[10] Según reza el mismo:

> *"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física*".

Las Administraciones Públicas deben prestar especial atención a este artículo al tratar este tipo de datos, ya que se requiere una base legal reforzada para su procesamiento.

- **Artículo 25:** Este artículo se centra en el principio de protección de datos desde el diseño y por defecto. Las Administraciones Públicas deben implementar medidas técnicas y organizativas apropiadas para garantizar que

[9] Reglamento General de Protección de Datos, pág 36. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf (fecha de última consulta: 12-07-2023).

[10] Reglamento General de Protección de Datos, pág 38. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf (fecha de última consulta: 12-07-2023).

se apliquen las salvaguardias adecuadas para proteger los datos personales desde el inicio del diseño de los sistemas y servicios.[11]

- **Artículo 32:** Este artículo, que establece la obligación de las Administraciones Públicas de garantizar la seguridad de los datos personales que procesan[12], dispone:

> "*...aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> ***a)** la seudonimización y el cifrado de datos personales;*
>
> ***b)** la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> ***c)** la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
>
> ***d)** un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*".

Las instituciones deben implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado, teniendo en cuenta los riesgos asociados al tratamiento y la naturaleza de los datos.

Estos son solo algunos ejemplos de los artículos del RGPD que las Administraciones Públicas deben tener en cuenta al tratar datos personales. Además,

[11] Reglamento General de Protección de Datos, pág 48. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf (fecha de última consulta: 12-07-2023).

[12] Reglamento General de Protección de Datos, pág 51. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf (fecha de última consulta: 12-07-2023).

existen disposiciones adicionales relacionadas con la notificación de violaciones de datos, los derechos de los interesados, las transferencias internacionales de datos y la responsabilidad de los responsables del tratamiento, entre otros aspectos.

Es importante destacar que el RGPD proporciona un marco general, y cada país de la Unión Europea puede establecer normativas específicas adicionales en su legislación nacional para adaptar y complementar el RGPD. Por lo tanto, es necesario analizar la legislación española, que se aborda en la siguiente sección 2.1.2 de este trabajo.

2.1.2 Legislación española aplicable a las administraciones públicas.

En el ámbito de las Administraciones públicas en España, la protección de datos está regulada principalmente por la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Esta ley desarrolla y complementa el Reglamento General de Protección de Datos (RGPD) en el contexto español, y establece las normas específicas que las Administraciones Públicas deben seguir al tratar datos personales. A continuación, se estudiará la citada legislación:

En primer lugar, se desarrolla el tratamiento de datos por parte de las Administraciones Públicas. La ley establece normas específicas para el tratamiento de datos personales por parte de las Administraciones Públicas y organismos públicos. Se definen los conceptos de responsables y encargados del tratamiento de datos en el contexto de las instituciones gubernamentales[13], y se establecen los principios y obligaciones que deben cumplir al recopilar, utilizar y almacenar datos personales.

En segundo lugar, se analiza lo concerniente a los derechos de las personas en relación con sus datos personales:[14] La LOPDGDD garantiza y regula los derechos

[13] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD). Preámbulo V. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf (fecha de última consulta: 12-07-2023).

[14] LOPDGDD, Título III, págs 18, 19 y 20. (fecha de última consulta: 12-07-2023).

de los individuos en relación con sus datos personales tratados por las Administraciones Públicas. Esto incluye el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición. Las Administraciones Públicas deben garantizar que las personas puedan ejercer estos derechos de manera efectiva y sin obstáculos.

En tercer lugar, los procedimientos y garantías para el ejercicio de los derechos[15]. La ley establece los procedimientos y garantías que las Administraciones Públicas deben seguir al recibir y gestionar las solicitudes relacionadas con el ejercicio de los derechos de protección de datos por parte de los ciudadanos. Se establecen plazos y mecanismos para responder a estas solicitudes de manera oportuna y efectiva.

Asimismo, medidas de seguridad y notificación de violaciones de datos[16]. La LOPDGDD establece la obligación de las Administraciones Públicas de implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales que procesan. Además, se establecen los procedimientos y requisitos para la notificación de violaciones de datos a la Agencia Española de Protección de Datos (AEPD) y a los individuos afectados, en caso de que se produzcan incidentes de seguridad.

Por último, se establecen las sanciones y medidas disciplinarias[17]. La ley regula sanciones y medidas disciplinarias en caso de incumplimiento de las obligaciones de protección de datos por parte de las Administraciones Públicas. Estas sanciones pueden incluir multas administrativas significativas[18], así como otras medidas correctivas y disciplinarias.

[15] LOPDGDD. (fecha de última consulta: 12-07-2023).

[16] LOPDGDD, Disposición Adicional Primera, pág. 54. (fecha de última consulta: 12-07-2023).

[17] LOPDGDD, Artículo 27, pág. 23. (fecha de última consulta: 12-07-2023).

[18] LOPDGDD, Artículo 72 y ss., págs. 42-48. (fecha de última consulta: 12-07-2023).

Específicamente, esta Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establece una serie de artículos, entre los que encontramos significativamente:

- **Artículo 9[19]:** "*1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.*

  Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

  2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad".

  Este artículo regula el tratamiento de datos personales especialmente protegidos, como aquellos que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, los datos genéticos o biométricos, entre otros. Establece las condiciones específicas bajo las cuales se puede llevar a cabo el tratamiento de este tipo de datos por parte de las Administraciones Públicas.

- **Artículo 12 y ss.[20]:** Estos artículos se centran en los derechos de los interesados y establece los procedimientos y garantías que las Administraciones Públicas deben seguir para asegurar el ejercicio efectivo de estos derechos. Estos derechos incluyen el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición. Asimismo, se

[19] LOPDGDD, págs. 17 y 18. (fecha de última consulta: 12-07-2023).

[20] LOPDGDD, Título III, Capítulo II págs. 18-20. (fecha de última consulta: 12-07-2023).

establece la obligación de las Administraciones Públicas de proporcionar información clara y concisa sobre los datos personales que tratan.

- **Artículo 31[21]:** *"Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.*

  El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

  Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro".

  Este artículo regula la obligación de las Administraciones Públicas de llevar un registro de actividades de tratamiento de datos. Establece los elementos que deben incluirse en dicho registro, como la identificación del responsable del tratamiento, las categorías de datos tratados, los destinatarios de los datos y los plazos de conservación. Esta obligación tiene como objetivo garantizar la transparencia y la rendición de cuentas en el tratamiento de datos por parte de las Administraciones Públicas.

- **Artículo 37[22]:** Este artículo se refiere a la figura del delegado de protección de datos (DPD) en el ámbito de las Administraciones Públicas. Establece las condiciones en las cuales las instituciones gubernamentales deben designar un DPD y define sus funciones y responsabilidades. El DPD es responsable de supervisar el cumplimiento de la normativa de protección de datos en las

[21] LOPDGDD, pág. 25. (fecha de última consulta: 12-07-2023).

[22] LOPDGDD, pág. 28. (fecha de última consulta: 12-07-2023).

Administraciones Públicas y actuar como punto de contacto con la Agencia Española de Protección de Datos (AEPD).

La legislación española, como se observa, busca complementar y transponer las disposiciones del RGPD a nivel nacional, proporcionando un marco legal específico para el tratamiento de datos personales por parte de las instituciones gubernamentales.

3. INTELIGENCIA ARTIFICIAL EN LAS ADMINISTRACIONES PÚBLICAS.

3.1 Introducción.

La aplicación de la inteligencia artificial (IA) en las Administraciones Públicas ha experimentado un crecimiento significativo en los últimos años, por ejemplo en el caso de los *chatbots* o en la automatización de procedimientos. La IA ofrece un amplio abanico de oportunidades para mejorar la eficiencia, la toma de decisiones y la prestación de servicios por parte de las instituciones gubernamentales. [23]

A continuación, se analiza el impacto de la inteligencia artificial en las Administraciones Públicas[24]:

- **Uso de algoritmos y análisis de datos:** Las Administraciones Públicas utilizan la IA para analizar grandes volúmenes de datos y obtener información relevante para la toma de decisiones. Los algoritmos de aprendizaje automático y la minería de datos permiten identificar patrones, predecir

[23] LARRAÑAGA, PEDRO. (2019). *"¿Es un Ministerio de Inteligencia Artificial una idea descabellada?"* - Fundación Telefónica. Universidad Politécnica de Madrid (UPM). Disponible en: https://www.fundaciontelefonica.com/noticias/por-que-un-ministerio-de-inteligencia-artificial-no-es-una-idea-descabellada/. (fecha de última consulta: 12-07-2023).

[24] VALERO TORRIJOS, J. (2019). «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración». Revista catalana de dret públic. Núm. 58, págs. 82-96. (fecha de última consulta: 12-07-2023).

comportamientos y optimizar los procesos internos de las instituciones públicas.

- **Mejora de servicios públicos:** La inteligencia artificial se utiliza para mejorar la prestación de servicios públicos, como la atención al ciudadano, la gestión de trámites administrativos y la planificación urbana. Los *chatbots* y asistentes virtuales proporcionan respuestas automáticas a consultas frecuentes, reduciendo la carga de trabajo del personal y mejorando la experiencia del usuario.

- **Automatización de tareas:** La IA permite automatizar tareas rutinarias y repetitivas en las Administraciones Públicas. Esto libera tiempo y recursos para que los funcionarios se concentren en actividades de mayor valor añadido, como el análisis de políticas públicas y la atención personalizada a los ciudadanos.

- **Detección de fraudes y prevención del delito:** Los algoritmos de IA pueden analizar grandes cantidades de datos para detectar patrones sospechosos y prevenir fraudes en áreas como la Seguridad Social, la fiscalidad o la contratación pública. Además, la inteligencia artificial también se utiliza en la identificación y prevención del delito, ayudando a las Fuerzas y Cuerpos de Seguridad del Estado a analizar datos y tomar decisiones más informadas.

- **Transparencia y rendición de cuentas:** La IA puede contribuir a mejorar la transparencia y la rendición de cuentas en las Administraciones Públicas. Mediante el uso de algoritmos explicables y la implementación de mecanismos de control, es posible garantizar que las decisiones automatizadas sean justas, imparciales y estén basadas en criterios objetivos.

Sin embargo, la implementación de la inteligencia artificial en las Administraciones Públicas también plantea desafíos y preocupaciones, especialmente en lo que respecta a la protección de datos personales y la ética, lo cual se desarrollará más adelante.

3.2 Conceptos clave y aplicaciones de la IA en el sector público.

En el contexto de la inteligencia artificial (IA) aplicada al sector público, existen conceptos clave y aplicaciones específicas que son relevantes para comprender su implementación y sus implicaciones, entre los que destacan:

El aprendizaje automático *(Machine Learning)*[25]: El aprendizaje automático es una rama de la IA que se basa en la capacidad de las máquinas para aprender y mejorar a partir de datos sin ser programadas explícitamente. En el sector público, el aprendizaje automático se utiliza para desarrollar modelos predictivos y clasificadores que permiten tomar decisiones informadas y anticiparse a posibles situaciones. Un ejemplo podría ser la predicción de necesidades de atención médica en sistemas de salud pública.

El procesamiento del lenguaje natural *(Natural Language Processing, NLP)*[26]: El procesamiento del lenguaje natural es una rama de la IA que permite a las máquinas comprender y procesar el lenguaje humano de manera natural. En el sector público, el NLP se utiliza para analizar grandes volúmenes de texto, como documentos legales o informes, y extraer información relevante. Un ejemplo sería el análisis automatizado de comentarios y quejas de los ciudadanos en redes sociales o portales de atención al cliente para identificar problemas recurrentes y mejorar la calidad de los servicios públicos.

La visión por computadora *(Computer Vision)*[27]: La visión por computadora es una disciplina de la IA que se centra en la capacidad de las

[25] YULU PI. (2021) "Machine learning in Governments: Benefits, Challenges and Future Directions". Disponible en: https://www.researchgate.net/publication/354111137_Machine_learning_in_Governments_Benefits_Challenges_and_Future_Directions (fecha de última consulta: 12-07-2023).

[26] Oracle. (2023). "What is Natural Language Processing?". Disponible en: https://www.oracle.com/hk/artificial-intelligence/what-is-natural-language-processing/ (fecha de última consulta: 12-07-2023).

[27] SuperAnnotate. (2022). "AI and computer vision in government". Disponible en: https://www.superannotate.com/blog/ai-and-computer-vision-in-government (fecha de última consulta: 12-07-2023).

máquinas para comprender y analizar imágenes y videos. En el sector público, la visión por computadora se utiliza para reconocer patrones, objetos y rostros, y tomar decisiones basadas en la información visual; tal como sucede con el uso de sistemas de reconocimiento facial en la seguridad pública para identificar a individuos sospechosos o buscar personas desaparecidas.

Los *chatbots* y asistentes virtuales: Son aplicaciones de IA que interactúan con los usuarios a través de lenguaje natural, brindando respuestas automáticas a preguntas frecuentes y realizando tareas simples. En el sector público, se utilizan para mejorar la atención al ciudadano y agilizar los procesos de comunicación, observándose en la implementación de *chatbots* en los sitios web de las Administraciones Públicas para proporcionar información sobre trámites administrativos, horarios de atención y requisitos legales.

La toma de decisiones automatizada: La IA también se utiliza en la toma de decisiones automatizada en el sector público. Mediante algoritmos y modelos avanzados, la IA puede analizar datos y proporcionar recomendaciones o decisiones basadas en criterios objetivos como, por ejemplo, en el uso de sistemas de IA para la asignación de recursos en áreas como la planificación urbana, la distribución de presupuestos y la gestión del tráfico, analizándolo mediante el proyecto JuLIA[28].

Por tanto, hay varias utilidades de la Inteligencia Artificial dentro del sector público: toma de decisiones automatizadas, *chatbots*, procesamiento de lenguaje natural, visión por computadora y aprendizaje automático.

[28] UNIVERSITAT POMPEU FABRA. (2023) "¿Cómo la inteligencia artificial y la toma de decisiones automatizada impactan en el ámbito jurídico?". Disponible en: https://www.upf.edu/es/inicio/-/asset_publisher/1fBlrmbP2HNv/content/com-la-intel%C2%B7lig%C3%A8ncia-artificial-i-la-presa-de-decisions-automatitzada-impacten-en-l-%C3%A0mbit-jur%C3%ADdic-/10193/maximized (fecha de última consulta: 12-07-2023).

3.3 Implicaciones legales y éticas de la inteligencia artificial en las Administraciones Públicas.

La implementación de la inteligencia artificial (IA) en las Administraciones Públicas plantea importantes implicaciones legales y éticas que deben abordarse de manera adecuada para garantizar el cumplimiento de los derechos de los ciudadanos y preservar los principios fundamentales del Estado de derecho. Además, desde una perspectiva española, se explorarán algunas de estas implicaciones y los desafíos asociados, tales como:

- **La privacidad y protección de datos:** La IA en el ámbito de las Administraciones Públicas implica el tratamiento de grandes cantidades de datos personales. En España, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) establece las obligaciones que deben cumplir las instituciones gubernamentales en relación con la recopilación, uso, conservación y seguridad de los datos personales. Es esencial garantizar que los sistemas de IA implementados cumplan con los principios de transparencia, minimización de datos y consentimiento informado expresamente. Además, se deben adoptar las medidas técnicas y organizativas necesarias para proteger la privacidad de los ciudadanos.[29]

- **La discriminación y el sesgo algorítmico:** Los algoritmos de IA pueden estar sujetos a sesgos inherentes en relación a los datos que obtiene y utiliza automáticamente para su entrenamiento, lo que puede llevar a decisiones discriminatorias o injustas. Para prevenir y mitigar el sesgo algorítmico, es fundamental que las Administraciones Públicas implementen salvaguardias adecuadas. Esto implica asegurar la transparencia en el diseño de los algoritmos, promover la diversidad en los conjuntos de datos utilizados y garantizar la supervisión humana en la toma de decisiones automatizadas.[30]

[29] ABITEBOUL, S., & DE GRANDA-ORIVE, J. I. (2020). Artificial intelligence, data protection and privacy law in Spain. In The Impact of Artificial Intelligence on Privacy págs. 73-92. (fecha de última consulta: 12-07-2023).

[30] CATERINA FALIERO, JOHANNA. (2021). "Limitar la dependencia algorítmica. Impactos de la inteligencia artificial y sesgos algorítmicos". Disponible en: https://biblat.unam.mx/hevila/Nuevasociedad/2021/no294/11.pdf (fecha de última consulta: 12-07-2023).

- **La responsabilidad y la rendición de cuentas**: La utilización de sistemas de IA en las Administraciones Públicas plantea la cuestión de la responsabilidad en caso de decisiones incorrectas o daños causados por errores o fallos en los algoritmos. Es necesario establecer mecanismos claros de responsabilidad y rendición de cuentas, identificando quién es responsable de las decisiones tomadas por los sistemas de IA y cómo se pueden corregir los posibles errores.[31]

- **La transparencia y la aplicabilidad de los sistemas de IA:** Son fundamentales para que los ciudadanos comprendan cómo se toman las decisiones en el ámbito de las Administraciones públicas. Los ciudadanos tienen derecho a entender qué datos y criterios se tienen en cuenta para llegar a una determinada decisión.

La implementación de la IA en las Administraciones Públicas debe guiarse por principios éticos y respetar los derechos fundamentales de los ciudadanos. Es esencial asegurar que los sistemas de IA se utilicen de manera justa, equitativa y conforme a los valores democráticos y los derechos humanos.

En España, la Agencia Española de Protección de Datos (AEPD)[32], desempeña un papel crucial en la supervisión y el cumplimiento de la normativa de protección de datos en relación con la implementación de la IA en las Administraciones Públicas. Además, a nivel europeo, se están desarrollando iniciativas como el Reglamento sobre la Inteligencia Artificial, que busca establecer un marco coherente y ético para el uso de la IA en diversos sectores, incluyendo el sector público.

Igualmente, se están empezando a desarrollar normativas dentro del ámbito autonómico como el **Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de**

[31] CRIADO, JUAN IGNACIO. (2021) "Inteligencia Artificial y Administración Pública". Disponible en: https://e-revistas.uc3m.es/index.php/EUNOM/article/view/6097/4426
(fecha de última consulta: 12-07-2023).

[32] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
(fecha de última consulta: 12-07-2023).

impulso a la inteligencia artificial en Extremadura y en la exposición de motivos se explica las novedades legislativas actuales en Europa y España y en concreto que:

> *"se ha dictado la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, que introduce la primera regulación positiva de la inteligencia artificial en España.*
>
> *Conforme al artículo 23 de la mencionada norma, las administraciones públicas que utilicen algoritmos para la toma de decisiones, favorecerán la puesta en marcha de mecanismos para que dichos algoritmos tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.*
>
> *En el caso de la Comunidad Autónoma de Extremadura la decisión de impulsar de forma decidida la IA no es caprichosa ni casual, sino que, por el contrario, supone un hito más en la voluntad firme y clara de avanzar en esta nueva revolución a todos los niveles, tanto en el ámbito de la actuación de la propia administración, como en el firme propósito de la Junta de Extremadura de imbuir de la misma a todas las políticas públicas".*

4. INTERSECCIÓN ENTRE PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL EN LAS ADMINISTRACIONES PÚBLICAS.

4.1 Desafíos y riesgos de protección de datos en la implementación de inteligencia artificial en el sector público.

En el contexto previo, se han abordado los desafíos y riesgos relacionados con la intersección entre la protección de datos y la inteligencia artificial en las Administraciones Públicas. Se ha discutido la importancia del consentimiento

informado expresamente, la mitigación del sesgo algorítmico, la transparencia en las decisiones de IA, la seguridad de los datos y la supervisión de los sistemas de IA. Es fundamental trabajar en colaboración y establecer marcos normativos sólidos para garantizar una implementación ética de la inteligencia artificial en el sector público.

4.2 Análisis de la adaptación de la legislación europea y estatal al contexto de la inteligencia artificial en las Administraciones Públicas.

El análisis de la adaptación de la legislación europea y estatal al contexto de la inteligencia artificial en las Administraciones Públicas revela los esfuerzos realizados para abordar los desafíos y riesgos asociados a esta intersección. A continuación, se examinará cómo ambas legislaciones han abordado esta cuestión.

4.2.1 Legislación europea.

Recientemente, la Unión Europea ha estado trabajando en la preparación de la primera Ley de Inteligencia Artificial del mundo. Esto se debe a las preocupaciones planteadas por el Centro para la Seguridad de la IA sobre posibles riesgos para la humanidad debido a esta tecnología. En este contexto, se aprueba un Reglamento que establecerá prohibiciones directas sobre ciertos tipos de IA, clasificándolos en distintos grados de riesgo: Inaceptable, Alto y Limitado.

En primer lugar, se prohibirán todas las IA capaces de manipular el comportamiento de personas vulnerables[33]. Suponiendo la existencia de un programa de IA diseñado para interactuar con pacientes con problemas de salud mental, como depresión o ansiedad. Este programa puede utilizar técnicas persuasivas para influir en las emociones y comportamientos de los pacientes, incluso sin su pleno conocimiento o consentimiento.

[33] 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 (En adelante, Ley de Inteligencia Artificial). Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF (fecha de última consulta: 12-07-2023).

El sistema de IA podría utilizar algoritmos sofisticados para identificar las vulnerabilidades emocionales de los pacientes y adaptar sus respuestas y supuestas recomendaciones de mejora de manera que busquen influenciar en su estado emocional o decisiones. Por ejemplo, podría utilizar técnicas de persuasión sutil para fomentar la adopción de ciertos medicamentos o terapias específicas, incluso si no son necesariamente las mejores opciones para el paciente.

En segundo lugar, se vetarán las Inteligencias Artificiales que establezcan un sistema de puntuación social, como aquellos que califiquen a las personas como aptas o no aptas en situaciones como entrevistas de trabajo[34]. Asimismo, se prohibirán las IA que utilicen sistemas de reconocimiento biométrico, como el reconocimiento facial[35]. Es importante destacar que tecnologías como *"Chat GPT"* no estarían directamente prohibidas, pero se considerarían de alto riesgo, lo que permitiría a los Estados miembros y a la UE evaluar su posible prohibición en el ámbito de la educación, la interpretación y aplicación de la ley o los procesos de selección de empleo.[36]

Estas medidas buscan establecer límites y regulaciones claras en el uso de la inteligencia artificial, especialmente en áreas sensibles donde pueden surgir riesgos éticos y sociales. La finalidad es garantizar un uso responsable y seguro de esta tecnología, protegiendo los derechos y la privacidad de las personas.

En este caso, y como nos estamos centrando en las Administraciones Públicas, estarán prohibidas las inteligencias artificiales que puedan realizar, por ejemplo, una manipulación para influir en las elecciones políticas. Considerando que se implemente un programa de IA que esté diseñado para analizar datos de redes sociales, generar contenido personalizado con el objetivo de influir en las opiniones y decisiones de los votantes, este estaría completamente prohibido por contravenir -una

[34] Ley de Inteligencia Artificial. (fecha de última consulta: 12-07-2023).

[35] Ley de Inteligencia Artificial. (fecha de última consulta: 12-07-2023).

[36] PARLAMENTO EUROPEO. (2023) "La Eurocámara, lista para negociar la primera ley sobre inteligencia artificial". Nota de Prensa. Disponible en: https://www.europarl.europa.eu/news/es/press-room/20230609IPR96212/la-eurocamara-lista-para-negociar-la-primera-ley-sobre-inteligencia-artificial (fecha de última consulta: 12-07-2023).

vez se apruebe y entre en vigor- la referida normativa europea que se encuentra en tramitación.

Este sistema de IA podría utilizar algoritmos de análisis de datos y aprendizaje automático para identificar patrones en el comportamiento y las preferencias de los usuarios en las redes sociales. A partir de estos patrones, la IA podría generar mensajes políticos adaptados a cada usuario, con el fin de persuadirlos o manipular su pensamiento en favor de una ideología concreta.

El programa de IA podría enviar mensajes o publicaciones en las redes sociales que apelen a las emociones, sesgos cognitivos o creencias de los usuarios, con el objetivo de influir en sus decisiones políticas. Podría utilizar técnicas de persuasión, como la repetición de mensajes clave, el uso de argumentos emocionales o la manipulación de información, con el fin de moldear las opiniones de los votantes.

Este tipo de manipulación de IA en el contexto de las Administraciones Públicas plantea serios problemas éticos y democráticos. Puede socavar la integridad de los procesos electorales y comprometer la toma de decisiones informadas por parte de los ciudadanos. Por tanto, es esencial establecer estas salvaguardias y este aspecto en la regulación.

4.2.2 Legislación española.

España abordó por primera vez la regulación de la inteligencia artificial a través del artículo 23 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, como se indicó anteriormente con el Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura, mientras se espera la aprobación definitiva del Reglamento de la Unión Europea sobre Inteligencia Artificial.

Este artículo establece directrices para las Administraciones Públicas que deseen incorporar la inteligencia artificial en sus procedimientos administrativos, las cuales incluyen la promoción de mecanismos que consideren criterios de minimización de sesgos, transparencia y rendición de cuentas en los algoritmos utilizados por las Administraciones Públicas, siempre que sea técnicamente factible.

También se prioriza la transparencia en el diseño e implementación de los algoritmos y la capacidad de interpretar las decisiones adoptadas por ellos.

Además, se fomenta el uso de la inteligencia artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo las recomendaciones de la Unión Europea en este ámbito. Por último, se busca promover un sello de calidad para los algoritmos utilizados.

Sin embargo, es importante destacar que el artículo tiene un carácter más programático que imperativo, lo que dificulta su cumplimiento. Además, genera inquietud el hecho de que los requisitos de transparencia y protección contra sesgos puedan ser obviados si existen limitaciones técnicas, lo que plantea interrogantes sobre la posibilidad de utilizar sistemas de inteligencia artificial basados en "black boxes", es decir, aquellas entradas y operaciones que no son visibles para el usuario u otra parte interesada, las cuales llegan a conclusiones o decisiones sin proporcionar ninguna explicación sobre cómo se llegaron a ellas.

Asimismo, el Consell ha aprobado la creación del Observatorio de la Inteligencia Artificial de la Comunitat Valenciana y, por tanto, el Decreto 85/2023, de 9 de junio, del Consell, de creación del Observatorio de la Inteligencia Artificial de la Comunitat Valenciana, el cual es un órgano colegiado y consultivo cuya finalidad es analizar y planificar el impacto de la inteligencia artificial en el entorno socioeconómico autonómico. Este Observatorio, dependiente de la Consejería competente en innovación tecnológica, tiene como objetivo promover el uso de la inteligencia artificial como motor de crecimiento sostenible, fomentando la productividad, eficacia y el desarrollo de nuevas industrias, siempre respetando los derechos fundamentales y la sostenibilidad.

También se enfocará en prevenir brechas sociales y promoverá la participación de todos los sectores relacionados con la inteligencia artificial, facilitando la comunicación con la Administración y actuando como canal de transmisión de necesidades y propuestas. Entre sus funciones destacan el asesoramiento en la planificación normativa, la facilitación de información y la promoción del uso de la

inteligencia artificial en la Comunitat Valenciana y su entorno tanto a Administraciones Públicas como al ciudadano.

4.3 Buenas prácticas y recomendaciones para garantizar la protección de datos en la implementación de inteligencia artificial en las Administraciones Públicas.

La Evaluación de Impacto en la Protección de Datos (en adelante, EIPD) es un proceso clave para evaluar los posibles riesgos y desafíos en términos de protección de datos que puedan surgir en la implementación de proyectos de IA en las Administraciones Públicas. Esta evaluación permite identificar y abordar proactivamente los riesgos, adoptando medidas de mitigación adecuadas para garantizar la protección de los datos personales involucrados.

La realización de la EIPD en el contexto de las Administraciones Públicas en España está regulada en el artículo 24 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Según este artículo, las autoridades y organismos públicos deben realizar una EIPD cuando el tratamiento de datos personales mediante el uso de tecnologías de IA pueda entrañar un alto riesgo para los derechos y libertades de las personas afectadas.

Además de la LOPDGDD, la propuesta de Reglamento de la Unión Europea sobre Inteligencia Artificial también establece disposiciones relacionadas con la evaluación de impacto en la protección de datos en el contexto de la IA como ya se ha expresado. Este reglamento, que ya se encuentra aprobado, establece un marco normativo específico y armonizado en toda la Unión Europea para el uso de la IA, incluyendo aspectos relacionados con la protección de datos y la evaluación de impacto.

5. LEGISLACIÓN CANARIA EN LAS ADMINISTRACIONES PÚBLICAS EN BASE A LA INTELIGENCIA ARTIFICIAL.

A través de una investigación y conversación con el Excelentísimo Cabildo Insular de Tenerife, se ha llegado a la conclusión que en las Islas Canarias,

actualmente, no se está llevando a cabo un proyecto específico relacionado con la Inteligencia Artificial (IA), pero se está poniendo énfasis en la protección de datos.

Existe una política de seguridad aprobada que establece las directrices y medidas necesarias para garantizar la seguridad de la información y la protección de los datos en el entorno organizacional.

En este sentido, se ha implementado un proceso de seguimiento y supervisión para asegurar la correcta implementación y cumplimiento de dicha política de seguridad. Se lleva a cabo un monitoreo constante para evaluar el nivel de seguridad de la información y detectar posibles vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos.

Para garantizar el cumplimiento de las exigencias establecidas en el Esquema Nacional de Seguridad, se están llevando a cabo diferentes acciones. En primer lugar, se ha proporcionado formación y capacitación al personal para concienciar sobre la importancia de la seguridad de la información y los procedimientos adecuados para su protección. Esto incluye la sensibilización sobre las buenas prácticas de seguridad, el manejo adecuado de los datos y el cumplimiento de las políticas establecidas.

Además, se han realizado cambios en la relación de puestos de trabajo para asegurar que exista personal designado y capacitado específicamente en temas de seguridad de la información. Se ha asignado personal responsable de supervisar y garantizar el cumplimiento de las medidas de seguridad establecidas, así como de implementar controles y procedimientos adecuados para proteger los datos de manera efectiva.

La implicación de las Jefaturas y el resto del personal es fundamental para asegurar el éxito de estas iniciativas. Se fomenta la participación activa de todos los miembros de la organización en la implementación de las medidas de seguridad y el cumplimiento de las políticas establecidas. Esto incluye la colaboración en la identificación de posibles riesgos y la adopción de medidas preventivas para mitigarlos.

6. SENTENCIA DEL TRIBUNAL DEL DISTRITO DE LA HAYA, C/09/550982/ HA ZA 18-388, DEL 5 DE FEBRERO DE 2020.

Hasta la fecha, solamente se ha registrado una decisión judicial en Europa que aborda el uso de algoritmos en la prestación de servicios. Esta resolución específica es la Sentencia emitida el 5 de febrero de 2020 por el Tribunal de Distrito de La Haya, la cual declaró como ilegal el algoritmo denominado SyRI, utilizado por el gobierno de los Países Bajos para combatir el fraude en el ámbito de la seguridad social. El tribunal de La Haya invalidó dicho algoritmo al considerar que no cumplía con las exigencias necesarias de proporcionalidad y transparencia, y además violaba el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.[37] En este artículo se describe*:*

> *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*
>
> *3. El respeto de estas normas estará sujeto al control de una autoridad independiente".*

En esencia, la sentencia estableció que el gobierno neerlandés no había diseñado el algoritmo de manera apropiada ni había proporcionado información suficiente sobre su funcionamiento. Esta falta de transparencia y claridad en el algoritmo resultaba perjudicial para la privacidad y los derechos fundamentales de los ciudadanos. El tribunal consideró que la interferencia generada por el uso del algoritmo en el ejercicio del derecho al respeto de la vida privada no era necesaria ni

[37] MOLINA HERMOSILLA, OLIMPIA. (2023). "Inteligencia artificial, Big Data y Derecho a la protección de datos de las personas trabajadoras". Disponible en: https://revistas.uma.es/index.php/REJLSS/article/view/16225/16626 (fecha de última consulta: 12-07-2023)

proporcional en una sociedad democrática, como lo requiere el artículo 8 del Convenio Europeo de Derechos Humanos.

La sentencia resaltó la importancia del principio de transparencia en la protección de datos, que se encuentra consagrado tanto en la Carta de los Derechos Fundamentales de la Unión Europea como en el Reglamento General de Protección de Datos que se ha visto en los primeros apartados de este Trabajo de Fin de Grado. En este caso, el tribunal concluyó que el gobierno holandés no había revelado públicamente el tipo de algoritmos utilizados en el modelo de riesgo ni proporcionado información suficiente sobre el método de análisis de riesgos empleado. Asimismo, la legislación aplicable al algoritmo no establecía ninguna obligación de informar a las personas cuyos datos eran tratados, lo que implicaba que los individuos no tenían conocimiento de que sus datos estaban siendo utilizados para tales fines. Además, no existía ninguna obligación de notificar individualmente a los interesados en caso de que su evaluación de riesgo resultara positiva.

Como resultado, el tribunal concluye que no es posible verificar el funcionamiento del algoritmo ni defenderse adecuadamente en caso de que se realice un informe de riesgos sobre una persona. En resumen, la sentencia destaca la falta de proporcionalidad, transparencia y protección de la vida privada en el sistema algorítmico utilizado por el gobierno holandés.

7. MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL (MINECO). SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL.

Como último apartado, es interesante desarrollar el Ministerio de Asuntos Económicos y Transformación Digital debido a la importancia actual de la digitalización de las Administraciones, así como la implementación de la inteligencia artificial.

El Ministerio de Asuntos Económicos y Transformación Digital es el departamento de la Administración General del Estado encargado de formular,

coordinar y ejecutar la política del Gobierno en temas económicos, apoyo a la empresa y reformas para mejorar el crecimiento potencial del país. [38]Además, desempeña un papel fundamental en la interlocución con la Unión Europea y otros Organismos Económicos y Financieros Internacionales. También es responsable de la política de telecomunicaciones y de **impulsar la transformación digital, especialmente en las Administraciones Públicas.**

Asimismo, su estructura orgánica se encuentra desarrollada en el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital[39] (en adelante, Real Decreto). Así, en su **artículo 1,** se encarga de desarrollar la organización general del departamento:

El Ministerio de Asuntos Económicos y Transformación Digital tiene la responsabilidad de presidir la Comisión Delegada del Gobierno para Asuntos Económicos (CDGAE), un órgano colegiado encargado de asegurar la coordinación y coherencia de las políticas económicas de los diferentes departamentos ministeriales con los criterios de la política económica.

Es importante destacar que las competencias atribuidas al Ministerio se entienden en coordinación con otros departamentos ministeriales, sin perjudicar las competencias que les corresponden.

El Ministerio cuenta con tres órganos superiores: la Secretaría de Estado de Economía y Apoyo a la Empresa, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y la que más interesa por el desarrollo de este trabajo, **la Secretaría de Estado de Digitalización e Inteligencia Artificial.** Estos órganos desempeñan un papel clave en el ámbito económico y de transformación digital.

---

[38] ADMINISTRACIÓN GENERAL DEL ESTADO. "Ministerio de Asuntos Económicos y Transformación Digital". Disponible en: https://transparencia.gob.es/transparencia/transparencia_Home/index/PublicidadActiva/OrganizacionYEmpleo/Funciones/Funciones-METD.html (fecha de última consulta: 12-07-2023).

[39] Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: https://www.boe.es/buscar/pdf/2020/BOE-A-2020-2739-consolidado.pdf (fecha de última consulta: 12-07-2023).

La Subsecretaría de Asuntos Económicos y Transformación Digital depende directamente del titular del Ministerio y juega un papel importante en el apoyo y la coordinación de las funciones del Ministerio.

Para brindar apoyo inmediato al titular del Ministerio, existe un Gabinete con una estructura orgánica y composición establecidas por la normativa correspondiente.

Además, el Ministerio también tiene bajo su adscripción como órgano colegiado la Autoridad Macroprudencial Consejo de Estabilidad Financiera (AMCESFI), cuya presidencia es ostentada por el titular del Ministerio. Esta entidad se encarga de supervisar y garantizar la estabilidad financiera del país.

También, el Ministerio cuenta con el Comisionado especial para la Alianza por la Nueva Economía de la Lengua, que tiene rango de Subsecretaría. Este Comisionado trabaja en el impulso de la economía relacionada con el idioma, en colaboración con los diferentes departamentos ministeriales.

Por otra parte, el **artículo 8** del Real Decreto describe la Secretaría de Estado de Digitalización e Inteligencia Artificial.

La Secretaría de Estado de Digitalización e Inteligencia Artificial, en el ámbito de sus competencias, ejerce diversas funciones relacionadas con la política de impulso a la digitalización de la sociedad y la economía, siempre respetando los derechos individuales y colectivos, así como los valores del ordenamiento jurídico español.

Entre las funciones específicas de la Secretaría de Estado se encuentran:

> *"a) Impulsar, programar y supervisar las acciones para la transformación digital e innovación de la Administración, a través de las tecnologías de la información y las comunicaciones, y adoptar soluciones digitales eficientes*

que permitan la prestación de servicios públicos de calidad, incluyendo los servicios públicos esenciales.

b) Crear servicios públicos electrónicos universales y de calidad, incluso aquellos que sean transfronterizos.

c) Fomentar la cooperación con otras administraciones públicas en materia de administración digital, promoviendo el uso de servicios de información para reducir la brecha digital y facilitar programas de atención al ciudadano. Además, impulsar el uso de plataformas comunes para integrar los servicios de diferentes sedes electrónicas de las administraciones públicas.

d) Proponer, coordinar y dar seguimiento a las relaciones internacionales en el ámbito de la sociedad digital, representando al Reino de España en colaboración con el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

e) Ejercer competencias relacionadas con la administración electrónica y los servicios públicos digitales, así como la incorporación de tecnologías de la información y comunicaciones en la Administración General del Estado y el sector público estatal. También se encarga de las facultades relacionadas con los nombres de dominio de Internet correspondientes a España (.es).

f) Planificar, coordinar, desarrollar e impulsar políticas, planes, programas, proyectos y acciones para incorporar la ciberseguridad en la transformación digital del sector privado y la ciudadanía. Esto se realiza en coordinación con otras agendas sectoriales de ciberseguridad de otros departamentos ministeriales, además de gestionar programas europeos e internacionales en esta materia.

g) Promover la definición de regulaciones y estrategias desde la administración para mejorar las políticas de ciberseguridad en el ámbito privado.

h) Supervisar, controlar e inspeccionar en materia de ciberseguridad y ciber-resiliencia de los servicios digitales, en colaboración con otros organismos competentes. Además, impulsa y coordina iniciativas para garantizar la confianza y seguridad digital, especialmente en la protección de menores y colectivos vulnerables, en el ámbito de competencia de la Secretaría de Estado de Digitalización e Inteligencia Artificial y en coordinación con el Instituto Nacional de Ciberseguridad.

i) Elaborar y proponer normativa sobre ciberseguridad y ciber-resiliencia para el sector privado, en colaboración con otros organismos y sectores afectados, con el objetivo de lograr una transformación segura de la economía y la sociedad.

j) Participar en comisiones, grupos de trabajo y otros foros nacionales, europeos e internacionales relacionados con la ciberseguridad.

k) Gestionar las ayudas y subvenciones públicas en el ámbito del Centro Nacional de Coordinación de Ciberseguridad (CNC)"

La Secretaría de Estado de Digitalización e Inteligencia Artificial es responsable de ejercer diversas funciones relacionadas con la digitalización de la sociedad y la economía. Bajo la dirección del Ministerio de Asuntos Económicos y Transformación Digital, se encarga de impulsar y regular los servicios digitales, promover la administración electrónica, coordinar y cooperar con otros departamentos ministeriales y Administraciones Públicas, y garantizar el respeto a los derechos individuales y colectivos, así como a los valores legales en el ámbito de la política económica.

Entre las funciones específicas de la Secretaría de Estado se encuentran:

- *Impulsar, supervisar y programar las acciones para la digitalización y la innovación en la Administración Pública, a través de las tecnologías de la*

información y comunicación, con el objetivo de mejorar la eficiencia en la prestación de servicios públicos.

- *Crear servicios públicos electrónicos universales y de calidad, incluyendo aquellos que puedan ser utilizados transfronterizamente.*

- *Promover la cooperación con otras administraciones públicas en materia de administración digital, reduciendo la brecha digital y fomentando el uso de plataformas comunes para la integración de servicios.*

- *Participar en la definición de estrategias y regulaciones en el ámbito internacional relacionadas con la sociedad digital, colaborando con el Ministerio de Asuntos Exteriores.*

- *Desarrollar políticas y programas para la incorporación de la ciberseguridad en la transformación digital del sector privado y la ciudadanía, coordinando con otros departamentos ministeriales y gestionando programas europeos e internacionales.*

- *Impulsar la mejora de las políticas de ciberseguridad en el entorno privado desde la administración.*

- *Supervisar, controlar e inspeccionar los servicios digitales en materia de ciberseguridad, así como promover iniciativas para garantizar la confianza y seguridad digital, especialmente en la protección de los menores y colectivos vulnerables.*

- *Elaborar y proponer normativa en materia de ciberseguridad y ciber-resiliencia para el sector privado, en colaboración con otros organismos y sectores afectados.*

- *Participar en comisiones y foros nacionales, europeos e internacionales relacionados con la ciberseguridad.*

- *Gestionar ayudas y subvenciones en el ámbito de la ciberseguridad y supervisar su ejecución técnica y económica.*

- *Ejercer la tutela del Instituto Nacional de Ciberseguridad de España y de la entidad pública empresarial Red.es, a través de la Secretaría de Estado.*

Estas responsabilidades y funciones son fundamentales para impulsar la digitalización y la inteligencia artificial en España, garantizando la seguridad y el desarrollo de la sociedad digital en todos los ámbitos.

Asimismo, **la Secretaría General de Administración Digital** que desarrolla el **artículo 9** del Real Decreto, es un órgano directivo encargado de dirigir, coordinar y ejecutar las competencias relacionadas con la transformación digital de la administración. Bajo la autoridad de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial, esta secretaría se encarga del desarrollo técnico y aplicación de las leyes y normativas relacionadas con el procedimiento administrativo común y el *funcionamiento del sector público por medios electrónicos desarrollado este funcionamiento*.[40]

Entre las competencias de la Secretaría General de Administración Digital se encuentran:

- Esquemas Nacionales de Seguridad e Interoperabilidad: La secretaría se encarga de las competencias relacionadas con los esquemas de seguridad e interoperabilidad en el ámbito de la Administración General del Estado y sus Organismos Públicos. Esto implica establecer políticas, coordinar y racionalizar las tecnologías de la información y las comunicaciones, y dirigir el Centro de Operaciones de Ciberseguridad.

- Medios y servicios comunes digitales: La secretaría es responsable de definir los medios y servicios comunes digitales, incluidos los declarados

[40] LABRADOR ORELLANA, M.A (2023). Trabajo Fin de Grado *"La Sede Electrónica en la Administración General del Estado (A.G.E): Identificación, Registro, Notificación y Verificación de Documentos*". Págs. 6-9. (fecha de última consulta: 12-07-2023).

compartidos, y de su provisión, explotación y gestión para todas las Administraciones Públicas.

- Acciones derivadas de planes de acción para la transformación digital: En coordinación con otros departamentos ministeriales, la secretaría se encarga de llevar a cabo las acciones que se deriven de los planes de acción para la implantación de estrategias nacionales e internacionales en el ámbito de la transformación digital.

Además de estas competencias generales, la Secretaría General de Administración Digital también tiene una serie de funciones específicas, que incluyen:

- *"Elaboración de la estrategia en materia de Administración Digital y Servicios Públicos Digitales de la Administración General del Estado y sus Organismos Públicos, así como del proceso de innovación y el establecimiento de las decisiones y directrices necesarias para su ejecución."*

- *"Actuar como órgano referente nacional e interlocutor ante organismos e instituciones europeas e internacionales en el ámbito de la Administración Digital".*

- *"Supervisar la ejecución de medidas específicas establecidas en los planes de acción departamentales en materia de Transformación Digital".*

- *"Elaboración, desarrollo, implantación y gestión del Catálogo de Medios y Servicios Comunes, incluidos los Compartidos".*

- *"Preparación de asuntos para diferentes comisiones y comités relacionados con la tecnología y la administración electrónica".*

El **artículo 9 bis** establece las funciones de la Dirección General de Digitalización e Inteligencia Artificial, que incluyen:

a) Elaborar y coordinar la Estrategia española de Inteligencia Artificial.

b) Desarrollar normativas y regulaciones en inteligencia artificial y tecnologías digitales.

c) Impulsar la investigación y desarrollo en inteligencia artificial.

d) Coordinar programas de transformación digital en sectores productivos.

e) Regular plataformas digitales y proteger la privacidad de la información.

f) Promover la capacitación y el talento digital.

g) Fomentar la creación de contenidos digitales y el desarrollo de empresas tecnológicas.

h) Facilitar el acceso y uso de servicios digitales y reducir las brechas digitales.

La Dirección General de Digitalización e Inteligencia Artificial cuenta además con cuatro subdirecciones generales, encargadas de diferentes áreas específicas dentro de su ámbito de competencia: La Subdirección General de Economía del Dato y Digitalización, la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales, la Subdirección General para la Sociedad Digital y la Subdirección General de Talento y Emprendimiento Digital.

Para finalizar, el **artículo 12** versa sobre la Subsecretaría de Asuntos Económicos y Transformación Digital. En primer lugar, entre las funciones principales se encuentran entre otros:

- Representación del Ministerio.
- Relaciones institucionales.
- Asesoramiento técnico.
- Asesoramiento jurídico.
- Impulso de la administración electrónica y tecnologías de la información.
- Gestión de sistemas de información.
- Coordinación del Plan de Recuperación, Transformación y Resiliencia.

En segundo lugar, se describe que la Secretaría General Técnica está directamente subordinada a la Subsecretaría.

En tercer lugar, dependen directamente de la Subsecretaría, con nivel orgánico de subdirección general, los siguientes órganos: Subdirección General de Recursos Humanos, Subdirección General de Administración Financiera y Oficialía Mayor, Inspección de Servicios, Subdirección General de Tecnologías de la Información y las Comunicaciones, Oficina Presupuestaria, Subdirección General de Comunicación y Subdirección General de Coordinación y Seguimiento de fondos europeos.

En cuarto lugar, se establece un Gabinete Técnico como órgano de apoyo a la Subsecretaría.

En quinto lugar, adscritos a la Subsecretaría, con rango de subdirección general, se encuentran la Abogacía del Estado, la Intervención Delegada de la Intervención General de la Administración del Estado y la Junta Asesora Permanente.

En sexto lugar, el organismo autónomo ICAC queda adscrito al Ministerio a través de la Subsecretaría.

En séptimo lugar, así como por último, la Inspección General del Ministerio de Hacienda depende funcionalmente de la Subsecretaría para el ejercicio de sus competencias.

8. CONCLUSIONES.

En el presente trabajo se ha realizado un análisis exhaustivo sobre la protección de datos en las Administraciones Públicas en el contexto de la implementación de inteligencia artificial (IA). A lo largo del estudio, se han examinado la legislación europea y estatal aplicable, los conceptos clave y aplicaciones de IA en el sector público, las implicaciones legales y éticas, así como las buenas prácticas y recomendaciones para garantizar la protección de datos.

En cuanto a la legislación comunitaria, se ha observado que el Reglamento General de Protección de Datos (RGPD) establece un marco jurídico sólido para la protección de datos en todas las áreas, incluidas las Administraciones Públicas. Se han identificado los principios y requisitos relevantes del RGPD, así como las obligaciones específicas que deben cumplir las Administraciones Públicas en el tratamiento de datos personales.

En el ámbito de la legislación estatal, se ha analizado la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), destacando su aplicación en las Administraciones Públicas. Se han detallado las disposiciones legales que afectan a estas entidades y las responsabilidades y obligaciones que deben cumplir en el tratamiento de datos personales.

En relación a la intersección entre protección de datos e inteligencia artificial, se han identificado los desafíos y riesgos que surgen en la implementación de la IA en el sector público. Se ha hecho hincapié en la necesidad de adaptar la legislación existente a este contexto, tanto a nivel europeo como español, y se ha señalado la importancia de la evaluación de impacto en la protección de datos (EIPD) en proyectos de IA.

En cuanto a las buenas prácticas y recomendaciones, se han presentado diversas medidas para garantizar la protección de datos en la implementación de IA en las Administraciones Públicas. Se ha resaltado la importancia de la evaluación de riesgos, la transparencia y aplicabilidad de los algoritmos utilizados, así como la seguridad y privacidad de los datos personales.

Este estudio ha permitido comprender la importancia de la protección de datos en el contexto de la implementación de inteligencia artificial en las Administraciones Públicas.

En conclusión, se ha evidenciado la necesidad de contar con una legislación actualizada y adaptada a los avances tecnológicos, así como de adoptar buenas prácticas que garanticen la seguridad y privacidad de los datos, debido a que estos aspectos actualmente son muy novedosos, teniendo competencia para ir interviniendo el Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Al seguir estas recomendaciones, las Administraciones Públicas pueden aprovechar los beneficios de la IA de manera responsable y ética, generando confianza en los ciudadanos y promoviendo un servicio público eficiente y justo.

9. BIBLIOGRAFÍA.

ZUBOFF, S, (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs. pág. 287

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). (2021). Guía de Protección de Datos y Privacidad en las Administraciones Locales. Disponible en: https://www.aepd.es/media/guias/guiaprivacidadentidadeslocales.pdf

GARCÍA-CAPELO, A., & GARCÍA, S. (2019). La protección de datos en las Administraciones Públicas: Un análisis a la luz del Reglamento General de Protección de Datos (RGPD). Ediciones Civitas.

Emilio GUICHOT (2005). Datos personales y Administración Pública. Madrid: APDCM-Thomson-Civitas. Pág. 230-234.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) (2020).Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento. Disponible en: https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf

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. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

LARRAÑAGA, PEDRO (2019) "¿Es un Ministerio de Inteligencia Artificial una idea descabellada?" - Fundación Telefónica, Universidad Politécnica de Madrid (UPM). Disponible en: https://www.fundaciontelefonica.com/noticias/por-que-un-ministerio-de-inteligencia-artificial-no-es-una-idea-descabellada/ .

VALERO TORRIJOS, J. (2019). «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración». Revista catalana de dret públic. Núm. 58, págs. 82-96.

YULU PI (2021) "Machine learning in Governments: Benefits, Challenges and Future Directions". Disponible en: https://www.researchgate.net/publication/354111137_Machine_learning_in_Governments_Benefits_Challenges_and_Future_Directions

ORACLE. (2023). "What is Natural Language Processing?". Disponible en: https://www.oracle.com/hk/artificial-intelligence/what-is-natural-language-processing/

SUPERANNOTATE. (2022). "AI and computer vision in government". Disponible en: https://www.superannotate.com/blog/ai-and-computer-vision-in-government

UNIVERSITAT POMPEU FABRA. (2023). "¿Cómo la inteligencia artificial y la toma de decisiones automatizada impactan en el ámbito jurídico?". Disponible en: https://www.upf.edu/es/inicio/-/asset_publisher/1fBlrmbP2HNv/content/com-la-intel%C2%B7lig%C3%A8ncia-artificial-i-la-presa-de-decisions-automatitzada-impacten-en-l-%C3%A0mbit-jur%C3%ADdic-/10193/maximized

ABITEBOUL, S., DE GRANDA-ORIVE, J.I. (2020). Artificial intelligence, data protection and privacy law in Spain. In The Impact of Artificial Intelligence on Privacy págs. 73-92.

FALIERO, JOHANNA CATERINA. (2021). "Limitar la dependencia algorítmica. Impactos de la inteligencia artificial y sesgos algorítmicos". Disponible en: https://biblat.unam.mx/hevila/Nuevasociedad/2021/no294/11.pdf

CRIADO, JUAN IGNACIO. (2021). "Inteligencia Artificial y Administración Pública". Disponible en: https://e-revistas.uc3m.es/index.php/EUNOM/article/view/6097/4426

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

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. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

PARLAMENTO EUROPEO "La Eurocámara, lista para negociar la primera ley sobre inteligencia artificial". Disponible en: https://www.europarl.europa.eu/news/es/press-room/20230609IPR96212/la-eurocamara-lista-para-negociar-la-primera-ley-sobre-inteligencia-artificial

ARAIZ HUARTE, DAVID EDGAR. (2022). "Primera regulación (y primera controversia) de la inteligencia artificial para el Sector Público español" LegalToday. Disponible en: https://www.legaltoday.com/practica-juridica/derecho-publico/publico/primera-regulacion-y-primera-controversia-de-la-inteligencia-artificial-para-el-sector-publico-espanol-2022-09-08/

KINZA YASAR. "black box AI", TechTarget. Disponible en: https://www.techtarget.com/whatis/definition/black-box-AI#:~:text=Black%20box%20AI%20is%20any,to%20how%20they%20were%20reached.

MOLINA HERMOSILLA, OLIMPIA (2023). "Inteligencia artificial, Big Data y Derecho a la protección de datos de las personas trabajadoras". Disponible en: https://revistas.uma.es/index.php/REJLSS/article/view/16225/16626

ADMINISTRACIÓN GENERAL DEL ESTADO. "Ministerio de Asuntos Económicos y Transformación Digital". Disponible en: https://transparencia.gob.es/transparencia/transparencia_Home/index/PublicidadActiva/OrganizacionYEmpleo/Funciones/Funciones-METD.html

Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: https://www.boe.es/buscar/pdf/2020/BOE-A-2020-2739-consolidado.pdf

LABRADOR ORELLANA, M.A. (2023). Trabajo Fin de Grado *"La Sede Electrónica en la Administración General del Estado (A.G.E): Identificación, Registro, Notificación y Verificación de Documentos"*.