Análisis comparativo de las tendencias y principios perseguidos en Occidente en materia de Inteligencia Artificial y su relación con la protección de los datos personales

Comparative analysis of the trends and principles pursued in the West regarding Artificial Intelligence and their relationship with the protection of personal data.

Alejandro Calvo de Mora Rivas[1], Mario Hernández Ramos[2]

RESUMEN

Este trabajo se centrará en el análisis comparativo de los principales textos legislativos sobre Inteligencia Artificial en Occidente, concretamente los desarrollados por la Unión Europea y el gobierno federal de Estados Unidos. Se comenzará con un enfoque en la protección de datos personales, dado que es un ámbito más consolidado normativamente y tiene una estrecha relación con la Inteligencia Artificial. Posteriormente, se abordará el análisis histórico y conceptual de la Inteligencia Artificial, para pasar al estudio detallado de los cuatro textos normativos seleccionados. El objetivo es determinar las tendencias y enfoques de ambos bloques occidentales en materia de Inteligencia Artificial, así como identificar posibles puntos de convergencia o divergencia entre ellos. Todo ello con la finalidad de analizar si priman los intereses económicos o la defensa de los derechos fundamentales de los ciudadanos en el desarrollo de la regulación de esta tecnología.

Palabras clave: Inteligencia Artificial, protección de datos personales, Legislación.

[1] CALVO DE MORA RIVAS, Alejandro. Universidad Complutense de Madrid, Facultad de Derecho, Derecho Constitucional, estudiante del Trabajo Fin de Grado. Curso académico: 2023-2024.
[2] HERNÁNDEZ RAMOS, Mario. Universidad Complutense de Madrid, Facultad de Derecho, Derecho Constitucional, Tutor del Trabajo Fin de Grado. Curso académico: 2023-2024.

ABSTRACT

This paper will focus on the comparative analysis of the main legislative texts on Artificial Intelligence in the West, specifically those developed by the European Union and the federal government of the United States. It will start with a focus on the protection of personal data, since it is a more consolidated area in terms of regulation and has a close relationship with Artificial Intelligence. Subsequently, the historical and conceptual analysis of Artificial Intelligence will be addressed, to move on to the detailed study of the four selected regulatory texts. The objective is to determine the trends and approaches of both Western blocs in the field of Artificial Intelligence, as well as to identify possible points of convergence or divergence between them. All this with the aim of analyzing whether economic interests or the defense of the fundamental rights of citizens prevail in the development of the regulation of this technology.

Keywords: Artificial Intelligence, Personal data protection, Legislation.

Introducción

La proliferación de la tecnología en nuestra sociedad ha generado la necesidad de su control y ha desencadenado en una obligación estatal y supraestatal de regularla para proteger los derechos de las personas en un marco donde se haga compatible la continuidad del desarrollo tecnológico y la salvaguarda de los derechos.

La tecnología no es una cosa sino un proceso, una capacidad de transformar o combinar algo ya existente para construir algo nuevo o bien darle otra función.

Cuando nos referimos al término tecnología es inevitable pensar directamente en las nuevas tecnologías que tienen un impacto tan grande en nuestras sociedades actuales, como puede ser la inteligencia artificial (en adelante, IA). No obstante, la IA es algo que ha ido poco a

poco formándose a lo largo de la historia, como expondremos en un apartado concreto, aunque en la actualidad bien es cierto que la IA es un tema de máximo interés social, intriga y preocupación, y sobre el cuál versará el contenido central de este trabajo.

A lo largo de la historia han sido innumerables las tecnologías que han ido creándose con una variedad y finalidades completamente diferentes las unas de las otras. Desde el desarrollo de tecnologías que facilitasen la difusión de la información como la imprenta, pasando por tecnologías que creasen una conexión instantánea entre las personas como internet y el acceso casi instantáneo a la información a través de ordenadores, teléfonos y otros dispositivos electrónicos, hasta llegar al tema de este análisis: la proliferación de la Inteligencia Artificial en Europa y EE. UU. en materia legislativa.

No podemos olvidarnos tampoco durante este análisis, dedicando un apartado específico para su análisis debido a la vital importancia de este y su estrecha relación con el desarrollo de la IA, de que todas estas tecnologías, siendo ahora más procedente comenzar a hablar dentro del marco de las – nuevas tecnologías –, a lo largo de los años, han ido recopilando una cantidad ingente de datos a nivel mundial y, por tanto, se creó la necesidad de comenzar a regular la distribución y gestión de estos datos. Ahora bien, cabe mencionar ahora que la regulación ha sido muy diferente en las distintas partes del globo, hasta el punto de ser considerado un DDFF en ciertas partes del mundo y en otras no, como veremos.

El contenido central de este trabajo estará centrado en un análisis de las diferentes tendencias, en el marco territorial de la civilización occidental, en materia de IA. Todo este análisis general de los principios y valores perseguidos se hará sobre la base de lo que bajo mi criterio son los cuatro textos legislativos más relevantes hasta la fecha en materia de IA en Occidente, desarrollados por la UE, el Consejo de Europa y el Gobierno federal de EE. UU.

Los textos estadounidenses que analizaremos son la *Blueprint for an Artficical Intelligence Bill of Rights*, centrado más bien es principios generales y constituyendo como unas pautas iniciales del desarrollo legislativo, y la *Executive Order 14110*, que nos reflejará más de cerca los ámbitos de aplicabilidad práctica de la legislación estadounidense en materia de IA. Utilizaremos ambos textos para posteriormente realizar una comparativa con las

regulaciones dadas en Europa en esta materia.

Para conocer las regulaciones europeas actuales en materia de IA nos centraremos en el análisis del *Artificial Intelligence Act*, norma de carácter reglamentario que nos mostrará la regulación más detallada y completa hasta la fecha en materia de IA, y la *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, tratado internacional formulado por el Consejo de Europa y con un carácter más general y de consenso global.

Finalmente, y para concluir, se dedicará un apartado final destinado a las conclusiones finales del análisis y posibles implicaciones a futuro de la materia. Para ello, utilizaremos el texto presentado por el Consejo de Europa, el cual, y como adelanto, versa como marco de convergencia entre ambos bloques contrapuestos en este análisis.

El trabajo dará comienzo con un análisis centrado en los datos personales y su protección. Comenzaremos con un enfoque conceptual, continuaremos con un análisis muy general acerca de las distintas tendencias que se han seguido hasta la fecha en materia de protección de datos y terminaremos con una referencia a la relación tan estrecha existente entre los datos personales y su protección con la IA.

Cabe destacar la vital importancia de este primer bloque en el análisis. Esto es debido a que hoy en día la regulación normativa existente en materia de IA es muy escasa y prácticamente inexistente, por tanto, partiremos desde una base más consolidada como lo es la protección de los datos personales. Mencionar, además, que es en el propio art.22 RGPD donde se menciona la implicación de la IA respecto a decisiones individuales automatizadas, incluida la elaboración de perfiles[3].

Posteriormente entraremos en el bloque de la IA. Abordaremos el análisis comenzando con un recorrido histórico, continuaremos con el análisis conceptual, pasaremos después al objeto central del desarrollo de este trabajo: los cuatro textos normativos referentes en el

[3] El 7 de diciembre de 2023 fue dictada la Sentencia SCHUFA en el TJUE, donde entra a ser sancionada una compañía de seguros alemana por precisamente la elaboración de perfiles. Para más información, consultar: https://acortar.link/l7iL9j

desarrollo legislativo en materia de IA bajo mi criterio, el cual dividiremos en dos partes y, para terminar, haremos unas conclusiones finales relativas al análisis comparativo de estos textos.

Este trabajo surge a raíz de las distintas experiencias personales durante mi formación académica, que derivaron en una profunda intriga acerca del mundo de las nuevas tecnologías y el tratamiento de los datos que estas generan y procesan. Durante mi breve período de prácticas voluntarias en la OTAN, mi preparación personal para poder acceder a másteres universitarios y mi viaje por trabajo en una universidad paraguaya, siempre he pensado en cómo podría implementarse esta idea de "inteligencia artificial" en estos ámbitos tan diferentes como: defensa, formación académica, economía, etc.

Debido a la complejidad del análisis técnico de la legislación específica para estos ámbitos tan amplios, decidí plantear un trabajo basado en un análisis más genérico centrado en EE. UU. y la UE. La razón es que otros países como China, que todos mencionan cuando nos referimos a IA, no persiguen un mismo enfoque en cuanto al concepto de derechos fundamentales y la protección de los ciudadanos respecto a los mismos. Es por ello por lo que el análisis versa en exclusiva sobre el bloque occidental, centrado en la defensa de los derechos fundamentales sobre la base del riesgo que generan estas nuevas tecnologías en los individuos, que actúan como eje central en ambas sociedades.

Para concluir este breve apartado, quiero dejar abiertas unas preguntas que intentaremos dar respuesta durante nuestra conclusión, una vez finalizado el análisis comparativo: ¿es realmente EE. UU. el país centrado únicamente en el crecimiento económico de sus empresas priorizando este sobre la defensa de los derechos fundamentales de sus ciudadanos? ¿estarán centradas las normativas estadounidenses en una regulación centrada en la empresa, el ciudadano o será mixta su intención? ¿seguirán la misma tendencia ambos bloques occidentales? ¿existe algún punto de convergencia entre ambos bloques?

Este tipo de preguntas, y las posibles múltiples respuestas que pueden plantear, han sido desde un inicio el motor que ha ido modulando el análisis de la investigación.

Los datos personales ¿Derecho fundamental?

La protección de datos es un concepto esencial en la era digital, donde la recopilación y el uso de información personal son omnipresentes. Este principio se originó como respuesta a las crecientes preocupaciones sobre la privacidad individual y la necesidad de salvaguardar la información personal de los ciudadanos. A lo largo del tiempo, ha evolucionado de ser un aspecto meramente secundario para convertirse en un componente esencial de los derechos fundamentales en muchas jurisdicciones, especialmente en la Unión Europea.

El origen de la protección de datos se remonta a las décadas de 1960 y 1970, cuando los avances tecnológicos permitieron una mayor automatización de la recopilación y procesamiento de información personal. Este cambio llevó a la necesidad de establecer normas y regulaciones para garantizar que los individuos mantuvieran el control sobre sus datos personales y que estos fueran tratados de manera justa y transparente.

La necesidad de protección de datos se sustenta en varios pilares. En primer lugar, la privacidad individual es un derecho humano fundamental, reconocido en diversas declaraciones y tratados internacionales. Además, el uso indebido de la información personal puede tener consecuencias perjudiciales, como el robo de identidad, el fraude o la discriminación. La protección de datos también fomenta la confianza en la sociedad digital, promoviendo un entorno en el que los individuos se sientan seguros al compartir información personal con otros usuarios privados o administraciones públicas

Las diferencias fundamentales en la conceptualización de la protección de datos entre la UE. y los EE. UU. han sido motivo de discusión y negociación. En la UE., la protección de datos personales es considerada un derecho fundamental. Esto se refleja en la legislación clave, como el RGPD., que otorga a los ciudadanos un control significativo sobre sus datos y establece estándares estrictos para las entidades que procesan información personal. Por otro lado, en los Estados Unidos, la protección de datos no se aborda de manera integral

como un derecho fundamental[4]. En lugar de contar con una legislación única y exhaustiva, la regulación se distribuye entre diversas leyes y agencias federales, lo que resulta en un enfoque más fragmentado y sectorial. La perspectiva estadounidense tiende a equilibrar la protección de datos con la promoción de la innovación y la economía digital.

Esta disparidad de enfoques ha llevado a tensiones en las relaciones comerciales y a la necesidad de mecanismos como el *privacy shield* [Escudo de Privacidad], dictado en la sentencia (Schrems I, 2015), aunque fue declarado ilegal en la sentencia (Schrems II, 2020), para facilitar la transferencia de datos entre la Unión Europea y los EE. UU. Sin embargo, las diferencias fundamentales persisten, y el diálogo continúa en busca de un equilibrio que garantice la protección de datos sin obstaculizar la innovación.

En conclusión, la protección de datos ha evolucionado desde su origen como respuesta a los avances tecnológicos hasta convertirse en un componente esencial de los derechos fundamentales. Las diferencias entre la Unión Europea y los EE. UU. residen en la consideración de la protección de datos como un derecho fundamental en la Unión Europea, mientras que en los EE. UU., se aborda de manera más fragmentada, equilibrando la protección con la promoción de la innovación. Estas divergencias plantean desafíos significativos en el ámbito internacional y subrayan la necesidad de un diálogo continuo para encontrar soluciones equitativas y efectivas.

Distintas tendencias a nivel mundial: marco legislativo

El desarrollo internacional de la protección de datos ha dado lugar a un complejo panorama global, donde diferentes regiones del mundo han respondido a la creciente importancia de la privacidad digital con enfoques y estrategias únicas y diferentes entre sí.

La cooperación internacional ha surgido como un elemento crucial en este panorama. Organismos como la OCDE y la ONU han reconocido la necesidad de establecer estándares globales para la protección de datos. Esta colaboración se manifiesta a través de foros y

[4] Para saber más acerca del concepto de datos personales utilizado en EE. UU. como "*personally identifable information*" acudir al siguiente texto legislativo: Circular No. A-130 - *Managing Information as a Strategic Resource.*

acuerdos, como la Comisión Internacional de Protección de Datos y Privacidad (ICDPPC) y el Foro de Cooperación Económica Asia-Pacífico (APEC), donde los países intercambian mejores prácticas y abordan desafíos comunes.

a. Europa

El Consejo de Europa, considerado por muchos expertos el paladín de la protección de datos, marcó un hito significativo en la protección de datos al promulgar el Convenio 108, el primer acuerdo internacional que aborda la protección de datos como un derecho fundamental. Esta iniciativa refleja el reconocimiento creciente de la importancia de salvaguardar la privacidad en la era digital a nivel global. El Convenio 108 establece principios fundamentales para la protección de la información personal, sentando las bases para futuras legislaciones y normativas en todo el mundo. Su adopción subraya la necesidad de enfoques unificados y principios comunes para garantizar la integridad y seguridad de los datos, consolidando la protección de la privacidad como un elemento esencial en el ámbito internacional.

La Unión Europea, en su caso, destaca como pionera en la creación de leyes robustas para la protección de datos. La implementación del Reglamento General de Protección de Datos desde su entrada en vigor el 24 de mayo de 2016 marcó un hito significativo, estableciendo estándares estrictos para el manejo de datos personales y otorgando a los individuos un mayor control sobre su información. Este reglamento fue publicado con el objetivo de concretar una directiva (Consejo, 24 de octubre de 1995) relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Posteriormente los distintos Estados de la UE. fueron promulgando sus respectivas leyes de protección de datos siguiendo los estándares de la UE., algunos ejemplos fueron:

a) España: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, de "06/12/2018".
b) Alemania: *Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097)*;

c) Francia: *loi n° 2018-493 du 20 juin 2018 relative à la protection des données personelles.*

b. Estados Unidos

En contraste, desde sus inicios, Estados Unidos ha adoptado una postura más flexible en cuanto al tratamiento de los datos personales, orientada hacia la libertad empresarial en lugar de hacia un control ciudadano más estricto. A diferencia de la Unión Europea, EE. UU. carece de una ley federal unificada; en su lugar, cada estado posee su propia legislación de protección de datos a la que se adhiere[5].

Tras la aprobación del Reglamento General de Protección de Datos y las presiones desde Europa para fortalecer las normativas, varios estados estadounidenses realizaron modificaciones en sus leyes o introdujeron cláusulas adicionales. Sin embargo, el cambio más significativo tuvo lugar en el verano de 2018, cuando California promulgó el California Consumer Privacy Act (CCPA), una medida sin precedentes en EE. UU. al imponer niveles de protección de datos muy similares a los del RGPD.

Desde entonces, varios estados han tomado medidas para actualizar sus leyes en este ámbito, y se anticipa que muchos más seguirán este camino. Hasta la fecha de julio de 2023, los estados que cuentan con leyes de protección de datos más completas y alineadas con el RGPD son: California, Colorado, Connecticut, Utah y Virginia[6]. Además, algunos estados adicionales han implementado diversas leyes estatales, aunque sin llegar al nivel de protección de los mencionados anteriormente.

c. Asia

China, por su parte, cuyas leyes históricamente se han centrado en el control estatal, promulgó la “Personal Information Protection Law" (PIPL), en 2021, la cual tuvo gran

[5] Analizaremos más a fondo la legislación estadounidense en materia de IA, y haremos breves menciones a las legislaciones en materia de protección de datos para completar este breve análisis.
[6] Para más información acerca de estas respectivas normas: 1) Colorado: The Colorado Privacy Act (CPA); 2) Connecticut: The Connecticut Data Privacy Act; 3) Utah: S.B. 227 Consumer Privacy Act; 4) Virginia: The Consumer Data Protection Act (CDPA).

alcance en las operaciones empresariales chinas.

A destacar de esta norma, la interpretación de "datos personales" e "información personal sensible" en la PIPL abarca cualquier información relativa a una persona física identificada o identificable, incluyendo datos de vídeo, voz o imagen. La exclusión de información anonimizada se establece claramente. La ley también define la "información personal sensible", abarcando datos biométricos, información religiosa, médica, direcciones de domicilios, información financiera y datos de menores de catorce años.

La PIPL de China, considerada por los expertos como una de las leyes más estrictas del mundo en materia de datos personales, establece restricciones para la recopilación y transferencia de datos, especialmente en aplicaciones que utilizan información personal para publicidad personalizada. Además, busca prevenir la transferencia de datos a países con políticas de seguridad o protección de datos menos estrictas.

En Singapur, la Ley de Protección de Datos Personales (PDPA) establece un estándar de protección para datos personales. La PDPA rige la recopilación, uso, divulgación y cuidado de estos datos, complementando marcos legislativos específicos de otros sectores. La ley busca el establecimiento de un Registro Nacional de No Llamadas (DNC) para que los individuos puedan optar por no recibir mensajes de telemarketing no deseados.

En Japón, la Ley de Protección de Información Personal (APPI) de 2003, revisada en 2017 y 2022, es la principal legislación que regula la recopilación y tratamiento de datos personales. La APPI establece la Comisión de Protección de Información Personal, un organismo regulador que emite pautas sobre la aplicación e interpretación de la ley. Se proporcionan directrices específicas para la transferencia de datos a terceros en países extranjeros.

En Corea del Sur, la Ley de Protección de Información Personal (PIPA) de 2011, modificada en 2023, regula la recopilación, uso y divulgación de datos personales. La privacidad, la privacidad de las comunicaciones y la libertad de expresión se reconocen como derechos fundamentales en la Constitución, y el consentimiento del titular de los datos es esencial para el tratamiento de sus datos.

En resumen, los Estados de Asia, como China, Singapur, Japón y Corea del Sur, han establecido marcos legales que definen y protegen los datos personales, pero varían en sus enfoques y requisitos específicos. Mientras China refuerza la protección y controla la transferencia internacional, Singapur busca equilibrar la protección interna con un registro de no llamadas. Japón y Corea del Sur han revisado sus leyes para fortalecer la regulación de la información personal, enfatizando el consentimiento del titular de los datos como un componente fundamental en el tratamiento.

d. Latinoamérica

La Red Iberoamericana de Protección de Datos (RIPD) surge como resultado de un acuerdo establecido durante el Encuentro Iberoamericano de Protección de Datos (EIPD) llevado a cabo en La Antigua, Guatemala, del 1 al 6 de junio de 2003. En este encuentro, participaron representantes de 14 países iberoamericanos, marcando el inicio de una colaboración regional en el ámbito de la protección de datos.

Uruguay y Argentina, en consonancia con su compromiso con estándares internacionales, se adhirieron al Convenio 108 del Consejo de Europa, subrayando su compromiso con la protección de datos a nivel global. Este hito ha favorecido a ambos Estados al ser, por tanto, considerados territorios donde existe seguridad en el tratamiento de los datos personales y es posible comercializar libremente con estos países, un hecho que ha favorecido al crecimiento económico de ambos Estados.

En Latinoamérica, varios estados han demostrado un interés activo en iniciativas relacionadas con la protección de datos. La creación de la RIPD responde a un anhelo compartido por las entidades participantes y se alinea con los acuerdos establecidos en la XXV Cumbre Iberoamericana de jefes de Estado y de Gobierno en Colombia en 2016[57]. En dicha cumbre, se solicitó a la Red la elaboración de propuestas para la cooperación efectiva en temas de protección de datos personales y privacidad.

[7] Para más información acerca de los asuntos tratados durante esta Cumbre: https://www.segib.org/wp-content/uploads/Recopilatorio-ES-Web-comprimido.pdf

En concordancia con estos objetivos, se han establecido los "Estándares de Protección de Datos de los Estados Iberoamericanos". Estos estándares representan un conjunto de directrices orientadoras destinadas a facilitar la formulación de iniciativas regulatorias sobre protección de datos personales en la región iberoamericana. Su propósito principal es proporcionar referencias para aquellos países que aún no cuentan con ordenamientos en este ámbito, al tiempo que sirven como guía para la modernización y actualización de las legislaciones ya existentes. De esta manera, los Estándares Iberoamericanos buscan consolidar un marco común que promueva la protección de la privacidad en la región.

e. África

En el continente africano, el impulso hacia la protección de datos se enfrenta a desafíos únicos dados los contrastes económicos y tecnológicos. Países como Nigeria y Sudáfrica han avanzado en la implementación de leyes específicas, pero la diversidad de la región plantea desafíos para lograr una aplicación efectiva en toda la región. Debido a su difícil análisis simplemente mencionaremos su existencia.

f. ¿Por qué un análisis de estas tendencias a nivel mundial?

Hemos analizado, aunque muy brevemente, las distintas regiones del globo en materia de protección de datos, pero ¿por qué? Esto tiene un sentido muy concreto, y es señalar con un ejemplo práctico que los grandes retos a los que la sociedad mundial se ha ido enfrentando a lo largo de la historia han sido objeto de muy diversas interpretaciones y valoraciones, las cuales en algunos puntos sí se alinean, pero en otros muchos llegan incluso a ser antagónicas.

Cuando nos referimos o intentamos analizar cada una de las distintas zonas del globo, es muy complejo precisar los rasgos legislativos concretos de cada una de las regiones sin haber realizado un análisis minucioso, algo muy complejo debido a las barreras de idioma, entendimiento de las estructuras sociales, contexto histórico y demás. Es por ello por lo que es muy importante hablar de tendencias para no caer en generalizaciones y sesgos.

¿Qué es esto de las tendencias? De manera muy resumida pueden explicarse como una serie de principios, pensamientos, protecciones y objetivos similares en unas zonas del territorio respecto a una materia concreta. Estas tendencias nos ayudan a entender con rasgos generales cómo una zona geográfica del globo está afrontando unos retos determinados. Es por ello por lo que durante todo nuestro análisis emplearemos en multitud de ocasiones este término.

Respecto al análisis anterior en materia de protección de datos, podemos observar una clara tendencia en el bloque occidental hacia un mayor proteccionismo y limitaciones específicas en materia de protección de datos. Se busca en este bloque occidental una cierta uniformidad en el tratamiento de los datos personales, los cuales en la UE son considerados como un DDFF y en los EE. UU. no. Observamos que pese a seguirse una misma tendencia pueden existir divergencias entre las distintas zonas que la conforman.

Por otro lado, podemos observar una tendencia creciente en Latinoamérica respecto al interés en crear una regulación, incluso común, en materia de protección de datos. Observamos cómo existen iniciativas de reunirse todos los Estados de manera conjunta y tratar de buscar unas líneas generales que sirvan como pauta a seguir para todos ellos, como por ejemplo los Estándares Iberoamericanos en Protección de Datos[8].

Respecto a Asia observamos una tendencia poco definida. Es cierto que sí existen textos legislativos que regulan los datos, pero los objetivos son completamente opuestos al bloque occidental y latinoamericano. En Asia se observa una tendencia que no parte de la base de la protección del individuo como centro de problema, sino más bien partidista y económica.

Este breve análisis comparativo será la base de nuestro posterior análisis en materia de IA, donde estas tendencias tan diversas se mantienen y el bloque occidental continúa siendo la pionera en legislación, incluso de manera más acentuada que respecto a los datos personales. Este breve análisis comparativo previo nos permite limitar el análisis del objeto del trabajo únicamente al marco legislativo occidental, y esto por dos razones: en primer

[8] Para saber más acerca de los estándares iberoamericanos: https://www.redipd.org/es/documentos/estandares-iberoamericanos

lugar, porque fuera del bloque occidental apenas aparecen intenciones realistas de crear una legislación pionera en materia de IA; y en segundo lugar, porque el bloque occidental, como ya hemos visto y volveremos a ver, sí parte de la base de la protección del individuo como centro del asunto y su tendencia es similar.

g. Relación con la IA

La intersección entre la protección de datos y la inteligencia artificial (IA) constituye un aspecto crucial en la era digital, donde los modelos fundacionales de IA desempeñan un papel central[9]. Estos modelos, basados en el procesamiento masivo de datos, presentan desafíos significativos relacionados con la interpretación y el sesgo. Es esencial reconocer que la calidad de los datos con los que alimentamos estos modelos puede impactar directamente en sus resultados, dando lugar a sesgos no deseados. Por ejemplo, si los conjuntos de datos utilizados para entrenar una IA contienen sesgos culturales o raciales, el modelo puede generar resultados discriminatorios ya desde sus orígenes.

La capacidad aparentemente ilimitada de las IA para procesar grandes cantidades de datos también plantea preocupaciones en términos de privacidad. Es imperativo establecer límites claros y conscientes en el acceso a determinados datos, evitando que las IA excedan sus funciones designadas, que son esencialmente de apoyo al ser humano. La adopción de medidas de protección de datos adecuadas se vuelve esencial para garantizar que la recopilación y el procesamiento de información se realicen de manera ética y respetuosa con la privacidad del individuo, que recordemos es esencial en un Estado social y democrático de derecho.

Es relevante destacar que, aunque los modelos fundacionales de IA pueden no ser tan numerosos a nivel mundial, las interfaces específicas que se desarrollan para cada uno de ellos multiplican su aplicabilidad. Un ejemplo claro es la creación de interfaces de idiomas para modelos como ChatGPT, que inicialmente se desarrolló en inglés y posteriormente se expandió para procesar y generar información en diversos idiomas. Esta adaptabilidad

[9] Para un entendimiento más extenso acerca de qué son los modelos fundacionales, leer el siguiente artículo del despacho PWC: https://ideas.pwc.es/archivos/20240301/que-son-los-modelos-fundacionales/

destaca la importancia de considerar las implicaciones culturales y lingüísticas al implementar sistemas de IA a escala global. Cabe destacar que estas interfaces están interconectadas las unas con las otras, es decir, si un individuo introduce textos de manera simultánea en ChatGPT en idiomas tan distintos como el chino, francés y alemán podrá observar cómo la IA redactará la información requerida en el idioma que solicite, sin importar el idioma en cual obtuvo la información.

En resumen, la relación entre la protección de datos y la IA se manifiesta en la necesidad de abordar los desafíos éticos y prácticos asociados con la recopilación, procesamiento y aplicación de datos en modelos fundacionales. La conciencia sobre el sesgo en los datos y la implementación de medidas de privacidad efectivas son esenciales para garantizar que la evolución de la IA se lleve a cabo de manera ética y equitativa.

Observaremos posteriormente, durante el análisis de las legislaciones estadounidenses y europeas materia de este análisis, que los textos normativos están destinados a paliar los daños que puede la IA provocar en la sociedad o el individuo, principalmente.

La Inteligencia Artificial: Cambio de paradigma

El tema central y sobre el cual los distintos agentes internacionales han estado centrados con una prioridad rotunda hasta hace unos pocos años, ha sido la recopilación y tratamiento de datos. Aunque esto no se queda aquí, dado que estos agentes también han buscado diversas opciones acerca de qué hacer con esos datos.

Ahora, con la entrada tan aplastante en nuestro marco de actualidad de la IA, el tema principal ha cambiado. Parece ser que el ciudadano promedio da por hecho que existen unos datos personales con los que las empresas y entidades estatales han estado haciendo distintas cosas durante mucho tiempo. Pero ahora mismo la información en sí no es el centro de atención, sino cómo unas máquinas pueden procesar estos datos y de qué manera.

Lo que llama tanto la atención de la IA es que como es capaz de procesar cantidades de datos de todo tipo en instantes, parece que es capaz de interpretar por sí misma la información.

Pongamos un ejemplo para explicar este punto de interés social. El teclado del ordenador que todos utilizamos a diario, ese que si presionamos una letra determinada nos introduce un carácter determinado en nuestra pantalla de forma automática, digamos que es una máquina "antigua". ¿Por qué? Porque un programador tuvo que diseñar que "cuando se pulse una tecla determinada habrá que proyectar un carácter determinado en la pantalla del dispositivo". Ahora bien, ¿qué tiene de diferente una IA? Lo diferente, y que tanto miedo e incertidumbre produce en las sociedades contemporáneas, es que detrás de estas IA no existe un programador que te diga "si esto, haz aquello", sino que los sistemas IA se entrenan sobre la base de las cantidades abrumadoras de información que establecen los resultados en base a probabilidades estadísticas que les lleva a inferir conclusiones del tipo "si este valor suma a ese valor, es muy probable que el resultado será aquel otro valor". Esta programación basada en probabilidad puede llegar a encontrar relaciones que no son obvias a primera vista. Por ello, parece que la IA es capaz de interpretar la información por sí misma y razonarla, aunque la realidad es que se basa en un mero procesamiento y retroalimentación basada en el tratamiento de información masiva.

La diferencia, en consecuencia, se centra entre la función determinista que se les atribuye a estas máquinas "antiguas" y la función estadística de las IA. Es decir, la IA determinará que lo estadísticamente más probable es que si pulsas una letra determinada nos de una imagen determinada en la pantalla del dispositivo, pero esto no será realizado de forma determinada sino probabilística.

En definitiva, el centro de atención versa hoy en día en las nuevas IA, en su desarrollo y utilidad práctica, pero sobre todo se encuentra en los perjuicios que esta puede provocar en los individuos de la sociedad mundial.

Terminar mencionando que lamentablemente no existe un consenso universal acerca del concepto propio de la IA, pero tanto la legislación europea como la estadounidense han otorgado su propia definición acerca del concepto de IA en sus respectivas legislaciones[10].

[10] Para conocer las definiciones explícitas acudir a: 1) UE.: al considerando 6), p. 22, en el siguiente enlace pdf: https://lc.cx/ig8Jp_ ; 2) EE. UU.: al apartado b), p. 3, en la orden ejecutiva dictada por la casa blanca objeto de este análisis: "Executive order 14110 of October 30, 2023".

Desarrollo histórico de la IA

En el siglo XIX, George Boole fue pionero en el desarrollo de la lógica matemática, un avance crucial que proporcionó la base teórica para la representación simbólica del conocimiento y la toma de decisiones en el ámbito de la inteligencia artificial (IA). Esta innovación allanó el camino para la conceptualización de sistemas lógicos que eventualmente se integrarían en el campo de la IA.

Más tarde, en la década de 1930, Alan Turing presentó la idea de una máquina universal, estableciendo los fundamentos teóricos de la computación y sentando las bases esenciales para el desarrollo posterior de la IA. La visión de Turing sobre las máquinas que podrían realizar cualquier cálculo posible sienta las bases conceptuales para los ordenadores modernos y, en última instancia, para el surgimiento de la inteligencia artificial en el siglo XX y más allá. Estos hitos tempranos demostraron ser fundamentales para el desarrollo de la inteligencia artificial y su impacto en la sociedad contemporánea.

En las décadas de 1950 y 1960, se presenció el surgimiento de las primeras implementaciones prácticas de la inteligencia artificial (IA). Inspiradas en la biología, las redes neuronales artificiales comenzaron a desarrollarse en los años 50, marcando un hito en la aproximación de las máquinas al funcionamiento del cerebro. En 1957, Frank Rosenblatt creó el Perceptrón, un modelo inicial de red neuronal que se convirtió en un precursor fundamental de las redes neuronales modernas.

Simultáneamente, se dio paso a la IA simbólica, destacando el desarrollo de sistemas basados en reglas lógicas. Un ejemplo notable fue el programa de ajedrez de IBM en 1956, que representó un avance significativo en la capacidad de las máquinas para abordar problemas complejos mediante la aplicación de reglas simbólicas. Estos hitos iniciales sentaron las bases para la convergencia de enfoques en la inteligencia artificial y marcaron el comienzo de una era de avances continuos en la aplicación práctica de estas tecnologías.

En las décadas de 1970 y 1980, la inteligencia artificial (IA) experimentó un período conocido como el "invierno de la IA", caracterizado por un descenso en el interés y la financiación. Este declive se atribuyó en gran medida a expectativas poco realistas sobre las

capacidades inmediatas de la IA. Sin embargo, a pesar de este período de desafíos, surgieron avances notables en la forma de sistemas expertos, entendidos como programas de ordenador diseñados para imitar la toma de decisiones de expertos humanos en un área específica y utilizan una base de conocimientos y reglas lógicas para resolver problemas en ese dominio.

Estos sistemas, fundamentados en reglas y conocimiento experto, destacaron en aplicaciones especializadas y marcaron un resurgimiento selectivo en el campo de la IA. A través de la focalización en áreas específicas y la aplicación de conocimientos expertos, los sistemas expertos allanaron el camino para el renacimiento posterior de la inteligencia artificial al ofrecer soluciones efectivas en contextos especializados.

Desde la década de 1990 en adelante, la inteligencia artificial (IA) ha experimentado un auge significativo, impulsado por diversos avances tecnológicos que han transformado la forma en que las máquinas procesan información y toman decisiones. El surgimiento del aprendizaje automático, a partir de los años 90, marcó un hito fundamental.

Enfoques como las máquinas de vectores de soporte y las redes neuronales profundas revolucionaron la capacidad de las máquinas para aprender patrones complejos y realizar tareas cognitivas avanzadas. Además, el acceso a grandes cantidades de datos y mejoras en el poder computacional se convirtieron en factores clave para el éxito continuo de la IA.

El fenómeno del "Big Data" proporcionó a los sistemas de IA conjuntos de datos extensos para el entrenamiento y la mejora de su rendimiento, creando así modelos fundacionales más precisos y concretos. Como resultado, la IA se ha integrado cada vez más en la vida cotidiana, manifestándose en asistentes virtuales, recomendaciones personalizadas y aplicaciones de reconocimiento de voz e imagen que han cambiado la forma en que interactuamos con la tecnología en nuestra rutina diaria.

El impacto social y económico de la inteligencia artificial (IA) ha sido significativo, marcando transformaciones profundas en diversos aspectos de la sociedad contemporánea.

La automatización de tareas impulsada por la IA también ha generado cambios laborales

sustanciales, afectando a múltiples sectores y sus modalidades de operación. La discusión sobre el futuro del trabajo se ha intensificado a medida que la IA se ha incorporado en procesos productivos, planteando preguntas sobre la reconfiguración de roles laborales y la necesidad de adaptación.

La transformación y adaptación de industrias es otro aspecto clave del impacto de la IA. Sectores como la salud, finanzas, manufactura y transporte han experimentado cambios significativos gracias a la implementación de soluciones basadas en inteligencia artificial. Desde diagnósticos médicos más precisos hasta sistemas financieros más eficientes, la IA ha demostrado su capacidad para mejorar la eficacia y la calidad en diversos ámbitos económicos.

Sin embargo, este rápido avance no está exento de preocupaciones éticas y desafíos. El debate en torno a la privacidad, el sesgo algorítmico y la responsabilidad en la toma de decisiones ha ganado prominencia con el aumento de la aplicación de la IA en la vida cotidiana. La necesidad de establecer marcos éticos y regulaciones sólidas se ha vuelto esencial para garantizar un desarrollo equitativo y responsable de la inteligencia artificial.

Textos legislativos estadounidenses

EE. UU. se ha proclamado como uno de los bloques pioneros a nivel internacional en el desarrollo de normas que regulen la implementación de las inteligencias artificiales dentro de la sociedad. Este análisis estará centrado en dos textos fundamentalmente, con breves menciones dentro de los distintos capítulos respecto a otras legislaciones federales y estatales en materia de IA. En primer lugar, se realizará un análisis del *Blueprint* [borrador], el cual actúa como una referencia que, sin estar en vigor, inspira el desarrollo de otros textos legislativos como la propia *Executive Order 14110* [orden ejecutiva], del 30 de octubre, que será analizada en segundo lugar La *Executive Order 14110* sí se trata de un texto en vigor en los EE. UU., siendo la aplicación más reciente en materia de IA realizada por el gobierno federal[119] de los EE. UU. Y esto será precisamente el objeto del análisis: observar de qué

[11] Este análisis no está centrado en el análisis del sistema territorial de los EE. UU., para más información consultar: https://lc.cx/eskRBX

manera, sobre la base de unos principios y objetivos, la Administración Biden busca aplicar y crear normativas en materia de IA.

Concluiremos este análisis, respecto a cada uno de los capítulos correspondientes a cada uno de los textos mencionados, con un breve análisis y desarrollo acerca de los aspectos más relevantes extraídos de cada texto.

a. *Blueprint for an AI Bill of Rights*

El borrador presentado se constituye como un faro en el panorama de la política tecnológica, destinado a dirigir los sistemas de inteligencia artificial hacia un propósito noble: el servicio efectivo y beneficioso para los ciudadanos estadounidenses. Este borrador fue emitido por la Oficina de la Casa Blanca de Política Científica y Tecnológica en el año 2022, y presenta un hito significativo dentro de un proceso continuo hacia la formulación de una "declaración de derechos para un mundo impulsado por la IA".

Su aparición responde a la necesidad apremiante de establecer directrices que aseguren que el avance vertiginoso de la IA se traduzca en progreso social y no en perjuicio de los derechos fundamentales. En su esencia, este texto servirá como un aliado en el desarrollo de políticas y prácticas que protejan la dignidad humana, salvaguarden los derechos civiles y fomenten principios democráticos en todas las facetas de la creación, implementación y supervisión de sistemas de inteligencia artificial. Sin embargo, es importante destacar que la implementación de los principios delineados en este documento no puede ser uniforme; debe adaptarse y modularse según las particularidades de cada contexto.

En el propio texto, además, se reconoce la complejidad inherente a las actividades de aplicación de la ley, donde se requiere un equilibrio delicado entre la seguridad pública y la protección de la privacidad y los derechos individuales. En este sentido, el borrador no solo busca establecer normas claras, sino también fomentar un diálogo continuo y una reflexión constante sobre los valores y principios que deben regir la era de la inteligencia artificial.

En el contexto actual, los Estados Unidos enfrentan una encrucijada crucial donde el uso de tecnologías emergentes, la gestión de datos y la implementación de sistemas de inteligencia

artificial plantean desafíos sin precedentes para los derechos y valores fundamentales del pueblo estadounidense. Esta coyuntura se percibe como una potencial amenaza al tejido mismo de la democracia, desafiando los cimientos sobre los cuales se fundó la nación, según puede entenderse tras el análisis del texto.

La administración de Joe Biden no se ha quedado al margen y ha proclamado que ni los valores democráticos ni los derechos civiles deben ser sacrificados en el altar del progreso tecnológico. Esto es interesante porque durante el desarrollo del texto se hacen múltiples menciones acerca de la protección empresarial y ciudadana en la implementación de IA, y de alguna manera da a entender que se centra más en una protección del individuo que meramente económica.

Cierto que es que la afirmación anterior no se menciona directamente, sino que se deja caer en cuestiones como que, en este sentido, se requiere un enfoque proactivo y multifacético que no solo impulse la innovación tecnológica, sino que también garantice que dichos avances no socaven los principios fundamentales sobre los cuales se sustenta la democracia estadounidense.

El documento en cuestión se fundamenta en la articulación de cinco principios fundamentales, los cuales son esenciales para orientar el diseño, uso y desarrollo de sistemas de automatización con el fin de salvaguardar los derechos de los ciudadanos estadounidenses en la era de la inteligencia artificial. Estos principios representan un marco conceptual sólido que busca garantizar que la implementación de tecnologías de IA no comprometa la integridad ni la dignidad de las personas. A través de la práctica aplicación de estos principios, se aspira a mitigar los riesgos inherentes al avance acelerado de la tecnología, asegurando que los derechos civiles y los valores democráticos no se vean menoscabados en el proceso de innovación y desarrollo. Estos principios no solo proporcionan una guía clara para los diseñadores y desarrolladores de sistemas de IA, sino que también establecen un estándar ético y moral que debe regir todas las actividades relacionadas con la automatización y la inteligencia artificial. En última instancia, el objetivo primordial de estos principios, según se indica con claridad, es garantizar que la IA se utilice como una herramienta para el bien común, enriqueciendo la vida de los ciudadanos

estadounidenses sin comprometer su libertad ni su autonomía.

Aunque no existe una articulación única y universal de los Principios Fundamentales para la Gestión de la Información (PIFI), estos han sido reconocidos como elementos esenciales en la legislación y políticas de privacidad de datos en todo el mundo. Estos principios, aunque no están codificados de manera uniforme, han sido incorporados en diversas normativas y marcos regulatorios para proteger los derechos y la privacidad de las personas en el contexto de la gestión de datos personales. Es importante destacar que estos principios no están limitados a un ámbito específico, como la privacidad, los derechos civiles o la ética, sino que abarcan una gama amplia de intereses y preocupaciones relacionadas con la protección de los individuos y la gestión de riesgos asociados con el tratamiento de datos personales en entornos digitales.

El marco propuesto se erige sobre la sólida base de cinco principios fundamentales, los cuales han sido destilados a partir de la experiencia empírica y el análisis práctico, derivados del uso de la inteligencia artificial hasta la fecha. Estos principios, concebidos como pilares esenciales, buscan garantizar que el desarrollo y la implementación de sistemas automatizados de IA no solo sean seguros y efectivos, sino también éticos y respetuosos de los derechos humanos.

En los últimos años, hemos sido testigos de avances modestos pero significativos en la respuesta a los desafíos planteados por el rápido avance de las tecnologías emergentes, especialmente en el ámbito de la inteligencia artificial. Algunos gobiernos estatales y locales han tomado la iniciativa de abordar estas cuestiones mediante la promulgación de legislación específica que busca regular el uso y desarrollo de tecnologías como la IA. Estas leyes buscan llenar vacíos legales y proporcionar un marco normativo claro para proteger los derechos y la privacidad de los ciudadanos en un entorno cada vez más digitalizado.

Algo muy destacable respecto al contenido introductorio de este texto es que contempla, además, que algunos tribunales han ampliado las protecciones legales existentes para abarcar las nuevas realidades planteadas por estas tecnologías emergentes. A través de decisiones judiciales y jurisprudencia innovadoras, se han sentado precedentes importantes que reconocen los derechos y las preocupaciones de las personas en relación con el uso de

la inteligencia artificial y otras tecnologías automatizadas. Estos fallos judiciales reflejan una comprensión creciente y una voluntad de adaptar el marco legal existente para abordar los desafíos únicos planteados por la rápida evolución tecnológica.

Para concluir con esta introducción acerca del contenido esencial y antes de entrar en un desarrollo respecto a cada uno de los cinco principios, es importante mencionar que este texto no se encuentra en vigor ahora mismo. Ahora bien, el análisis de este es fundamental porque se erigió como la base esencial acerca de la concepción e interpretación de la IA y, además, ha sido la norma referencial en posteriores desarrollos normativos en el marco legislativo de EE. UU, algo que puede comprobarse debido a las múltiples citas existentes en los textos posteriores hacia este.

Vamos ahora a pasar a analizar brevemente los aspectos más destacados de cada uno de los cinco principios recopilados en este borrador, y lo haremos siguiendo la metodología adoptada por la propia Casa Blanca. En cada caso, nos centraremos en tres aspectos clave: 1) la importancia del principio; 2) las expectativas respecto a los sistemas de IA en relación con ese principio; 3) cómo se pueden implementar estos principios en la práctica.

Es importante tener en cuenta que, en esta breve aproximación, nos enfocaremos principalmente en el tercer punto, que aborda la implementación práctica de los principios en el mundo real. Por lo tanto, es posible que no desarrollemos completamente cada sección respecto a cada uno de los principios y centremos más la atención en los aspectos más relevantes y de aplicabilidad práctica.

b. Primer principio: sistemas seguros y eficaces (*safe and efective systems)*

En primer lugar, se postula la necesidad de asegurar la seguridad y eficacia de los sistemas de IA, para evitar potenciales riesgos y daños tanto a nivel individual como social. Esta premisa se convierte en un fundamento ético, considerando el impacto que estas tecnologías pueden tener en la vida cotidiana de las personas y en la estabilidad de las comunidades.

Para garantizar la seguridad y eficacia de los sistemas de IA, según este primer principio, es fundamental implementar salvaguardias proactivas y continuas. Esto implica consultar

al público en todas las fases del ciclo de vida del sistema, desde el diseño hasta el mantenimiento. Antes de su despliegue, los sistemas deben someterse a pruebas exhaustivas para identificar y mitigar los riesgos potenciales, centrándose en los derechos y oportunidades de las personas, así como en los riesgos para las comunidades afectadas. La supervisión continua es esencial, incluyendo la evaluación constante de los indicadores de rendimiento y la calidad de los datos utilizados. Además, los sistemas deben diseñarse para permitir la evaluación independiente, con acceso a datos asociados y reportes actualizados periódicamente que detallen la visión general del sistema y los datos utilizados. En resumen, la seguridad y eficacia de los sistemas de IA requiere consultas públicas, pruebas exhaustivas, supervisión continua y acceso a la información relevante para garantizar su funcionamiento adecuado y proteger los derechos de las personas.

Por ejemplo, imaginemos que una empresa está desarrollando un sistema de IA para la detección de fraudes financieros. En todas las etapas del desarrollo, desde el diseño hasta el despliegue, la empresa consulta a expertos en seguridad financiera, así como a grupos de defensa del consumidor y otras partes interesadas, para garantizar que el sistema sea seguro y ético. Antes de su lanzamiento, el sistema se somete a rigurosas pruebas de rendimiento y seguridad, identificando y abordando posibles sesgos o riesgos. Una vez implementado, el sistema se monitorea continuamente para evaluar su efectividad y mitigar cualquier problema que pueda surgir. Los informes periódicos detallan el funcionamiento del sistema y los datos utilizados, proporcionando transparencia y asegurando la rendición de cuentas.

Algunos estados han implementado estrictos requisitos de transparencia y equidad en el uso de evaluaciones de riesgo previo al juicio, lo que ha generado preocupaciones entre los grupos de derechos civiles. Por ejemplo, el Código de Idaho, en su artículo 19-1910 promulgado en 2019, exige que las evaluaciones de riesgo previo al juicio demuestren estar libres de prejuicios contra grupos protegidos por la ley estatal o federal. Además, requiere que toda la documentación utilizada en estas evaluaciones esté disponible para inspección pública y prohíbe el uso de secretos comerciales para justificar la discriminación en el proceso penal.

c. Segundo principio: protecciones contra la discriminación algorítmica

(algorithmic discrimination protections)

En segundo lugar, se aborda la cuestión crucial de las discriminaciones algorítmicas, reconociendo que los sistemas de IA pueden perpetuar y amplificar sesgos y prejuicios existentes en los datos y algoritmos utilizados. Por lo tanto, se establece la necesidad de implementar protecciones robustas que mitiguen estas injusticias y promuevan la equidad y la justicia social en el diseño y aplicación de sistemas automatizados.

Según este principio los sistemas automatizados deben ser probados para garantizar su libertad de discriminación algorítmica, con diseño equitativo y conformidad con la legislación antidiscriminación. Las evaluaciones deben ser inclusivas, considerando una amplia gama de grupos desatendidos, como personas de color, minorías religiosas, mujeres, LGBTQI+, personas mayores, personas con discapacidad, entre otros. Los datos utilizados deben ser representativos y revisados para detectar sesgos, y se deben implementar medidas para evaluar y mitigar las disparidades. Se requiere supervisión continua para detectar y abordar la discriminación algorítmica, y se deben proporcionar informes claros sobre la evaluación del impacto algorítmico y las medidas correctivas necesarias.

Debemos señalar varios ejemplos: 1) combatiendo la discriminación en préstamos hipotecarios: el gobierno federal está implementando medidas para combatir la discriminación en los préstamos hipotecarios, trabajando con agencias federales para garantizar la equidad en el acceso a la vivienda.; 2) identificando sesgos en el sistema de asistencia sanitaria: las evaluaciones de disparidad revelaron sesgos en el acceso a la atención médica para pacientes negros. Un algoritmo de asistencia sanitaria basado en el historial de atención médica pasada discriminaba a los pacientes negros, lo que resultaba en menos intervenciones médicas para ellos en comparación con los pacientes blancos con necesidades similares; 3) estableciendo estándares para gestionar sesgos en la IA: el NIST ha publicado la publicación especial 1270, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. Esta publicación aborda los desafíos de la parcialidad en la inteligencia artificial, identificando categorías de sesgos y proporcionando orientación sobre cómo mitigarlos, adoptando una perspectiva sociotécnica para identificar

y gestionar los sesgos de la IA.

d. Tercer principio: privacidad de los datos *(data privacy)*

En tercer lugar, se enfatiza la importancia de la protección de datos y la privacidad en el contexto de la IA, reconociendo que el uso indebido o la exposición no autorizada de información personal pueden erosionar la confianza pública en estas tecnologías y socavar los derechos individuales de privacidad. En este sentido, se insta a adoptar medidas proactivas para garantizar la confidencialidad y la integridad de los datos, así como para promover prácticas de transparencia y rendición de cuentas en el manejo de la información personal.

En este principio se refleja que la privacidad de los datos personales es un principio clave para garantizar otros aspectos dentro del marco legislativo. La legislación federal no ha evolucionado al ritmo de la creciente recopilación de datos y acceso gubernamental, lo que deja a los ciudadanos sin control sobre sus propios datos. A menudo, los intermediarios de datos recopilan información sin consentimiento. A pesar de algunos esfuerzos empresariales y estatales para abordar este problema, aún no hay un estándar claro ni un marco legal completo en los Estados Unidos para regular la protección de datos personales.

Los sistemas automatizados deben priorizar la privacidad desde su diseño inicial, con evaluaciones continuas de riesgos. La recopilación y uso de datos para entrenar modelos de aprendizaje automático deben ser legales y transparentes para los usuarios. La vigilancia solo se justifica cuando sea estrictamente necesaria y proporcional. Los derechos civiles no deben ser comprometidos por la vigilancia automatizada. El consentimiento debe ser claro, específico y limitado en tiempo y contexto. Las personas deben tener acceso y control sobre sus datos, con la capacidad de corregirlos. La transparencia y la evaluación independiente de las políticas de datos son esenciales, con respuestas rápidas a las solicitudes de información por parte de los usuarios.

La protección de datos en áreas sensibles como la salud, el empleo, la educación, la justicia penal y las finanzas personales es crucial para preservar la integridad y los derechos individuales. Los sistemas automatizados que operan en estos ámbitos deben cumplir expectativas adicionales, ya que las actividades realizadas pueden tener consecuencias

significativas en términos de derechos humanos y civiles. Ejemplos preocupantes ilustran cómo la falta de regulación puede llevar a la explotación de datos, como en el caso de dispositivos médicos cuyos datos se utilizan para negar cobertura de seguro, o análisis predictivos que revelan información personal sin consentimiento. Tales prácticas subrayan la necesidad urgente de salvaguardar la privacidad en estos contextos críticos.

Los datos sensibles solo deben ser utilizados para funciones estrictamente necesarias dentro de su ámbito correspondiente, y cualquier uso que pueda limitar derechos o oportunidades debe someterse a una revisión ética exhaustiva. Además, estos datos no deben ser vendidos, compartidos ni hechos públicos como parte de acuerdos de intermediación de datos.

Por ejemplo, la Ley de Privacidad de 1974 en EE. UU. establece la protección de la información personal en los sistemas de registros federales, asegurando límites en la retención de datos y proporcionando a los individuos el derecho de acceso y corrección de sus datos. En otro caso, ante el intento de un consejo escolar de vigilar a los alumnos de las escuelas públicas en Lockport, Nueva York, sin la adecuada participación comunitaria, se implementó una moratoria estatal sobre la biometría en las escuelas públicas hasta el 1 de julio de 2022, en respuesta a la legislatura estatal que prohibió el uso de sistemas de reconocimiento facial y otras "tecnologías de identificación biométrica".

e. Cuarto principio: notificación y explicación *(notice and explanation)*

El cuarto principio se centra en la necesidad de proporcionar notificación y explicación claras sobre el funcionamiento y las decisiones tomadas por los sistemas de IA. Esta transparencia es esencial para empoderar a los usuarios y garantizar que puedan comprender y cuestionar el funcionamiento de estos sistemas, así como para facilitar la detección y corrección de posibles errores o sesgos algorítmicos.

Los sistemas de inteligencia artificial deben ofrecer, de manera preceptiva, avisos de uso claros, oportunos y comprensibles, así como explicaciones sobre las decisiones o acciones que realizan. Es esencial que los usuarios reciban notificaciones antes de interactuar con la tecnología o mientras se ven afectados por ella, asegurando que las explicaciones estén disponibles junto con la decisión o poco después. Estas explicaciones deben adaptarse a la

finalidad específica para la que se espera que el usuario las utilice, garantizando una comprensión clara de la razón detrás de cada acción tomada por el sistema. Además, para gestionar adecuadamente los riesgos asociados con estos sistemas, es fundamental llevar a cabo evaluaciones que determinen su nivel de riesgo, lo que ayuda a informar sobre las medidas de mitigación necesarias y a promover una mayor transparencia en su funcionamiento.

f. Quinto principio: Alternativas humanas, consideración y repliegue *(human alternatives, consideration and fallback)*

Finalmente, el quinto principio subraya la importancia de promover alternativas humanas y la capacidad de retroceso en el desarrollo y aplicación de la IA. A pesar de los avances tecnológicos, se reconoce que la intervención humana sigue siendo indispensable en numerosos contextos, especialmente en aquellos que implican decisiones críticas que afectan a los derechos y el bienestar de las personas. Por lo tanto, se enfatiza la necesidad de diseñar sistemas de IA que complementen y fortalezcan la labor humana, en lugar de reemplazarla por completo, y que cuenten con mecanismos efectivos para corregir posibles desviaciones o errores.

Las personas pueden evitar los sistemas automatizados debido a problemas como fallos, sesgos o inaccesibilidad, subrayando la importancia de contar con alternativas humanas. En ámbitos sensibles como la justicia penal o la salud, donde se emplean sistemas automatizados, es esencial implementar salvaguardias y una supervisión humana rigurosa para evitar resultados injustos o peligrosos. Por ejemplo, en los centros de llamadas automatizados, mantener una opción de comunicación con un operador humano garantiza asistencia efectiva en situaciones complejas.

La formación sobre los sistemas automatizados es crucial para aquellos que los administran, interactúan o interpretan sus resultados, asegurando una comprensión adecuada y la capacidad de mitigar sesgos y efectos no deseados. Es importante reconocer que los sistemas basados en humanos pueden tener sesgos y limitaciones, especialmente en ámbitos sensibles como la atención médica o la justicia penal.

Por ejemplo, en el sector de la atención al cliente, la integración exitosa de servicios automatizados como los chat-bots y los sistemas de respuesta de llamadas basados en IA, con escalado a un equipo de asistencia humana, ha permitido a las empresas proporcionar una atención al cliente más rápida y efectiva. La combinación de IA y agentes humanos se considera esencial para el éxito en este campo, asegurando respuestas rápidas a consultas simples mientras se mantiene la capacidad de abordar solicitudes más complicadas con un enfoque humano.

g. *Executive order 14110 of October 30, 2023*

En la era actual, la IA emerge como una fuerza transformadora que promete remodelar fundamentalmente nuestro mundo en una variedad de aspectos, desde la productividad hasta la seguridad nacional. Sin embargo, esta promesa está acompañada de desafíos significativos. La Orden Ejecutiva 14110, emitida por la Administración Biden de los Estados Unidos el 30 de octubre de 2023, reconoce este equilibrio delicado entre el potencial extraordinario y los riesgos considerables asociados con la IA.

El objetivo fundamental de esta orden ejecutiva es abordar este desafío dual: aprovechar los beneficios de la IA para el bien común mientras se mitigan los riesgos potenciales que esta tecnología puede engendrar. La IA, cuando se utiliza de manera responsable, tiene el poder de resolver problemas apremiantes y fomentar un mundo más próspero, seguro e innovador. Sin embargo, un uso irresponsable podría amplificar problemas sociales como el fraude, la discriminación y la desinformación, así como erosionar el poder de los trabajadores y desestabilizar la competencia económica.

Este enfoque hacia la IA seguro y responsable no puede ser abordado únicamente por un sector de la sociedad; requiere una colaboración integral entre el gobierno, el sector privado, las instituciones académicas y la sociedad civil. La máxima urgencia otorgada por la Administración Biden refleja la necesidad crítica de una gobernanza y legislación efectivas de la IA, que garantice su desarrollo y uso en beneficio de la humanidad, al tiempo que se minimizan los riesgos asociados. En este contexto, se promueve un enfoque coordinado en todo el Gobierno Federal para llevar a cabo esta tarea monumental.

Es esencial para la Administración Biden avanzar en la gobernanza de la IA según ocho principios rectores y prioridades.

Recordemos que en el Blueprint analizado previamente se destacan cinco principios rectores, los cuales, aunque no estén expresados con la misma terminología y exactitud en todos los proyectos legislativos a nivel mundial y sirven como una guía mundial y son seguidos por la práctica totalidad de actores internacionales.

Respecto a esta orden ejecutiva[12] cabe esperar un análisis práctico acerca de cómo EE.UU. plantea "en su día a día" la aplicación normativa en materia de IA. Es importante mencionar que no analizaremos todos los principios de manera exhaustiva, sino que haremos un breve resumen de cada uno de ellos y en un apartado final nos centraremos en los temas más interesantes a tratar en la orden ejecutiva.

h. Análisis breve de los principios y prioridades

En primer lugar, se afirma que la Inteligencia Artificial debe ser segura. Este principio destaca la importancia de asegurar que los sistemas de IA sean seguros mediante evaluaciones sólidas y estandarizadas. Se enfatiza la necesidad de abordar los riesgos de seguridad, incluidos aquellos relacionados con la biotecnología, la ciberseguridad y la infraestructura crítica. Las pruebas y evaluaciones continuas son fundamentales para garantizar que los sistemas de IA funcionen de manera segura y como se espera.

En segundo lugar, se contempla el objetivo de promover la innovación responsable, la competencia y la colaboración. Este objetivo busca crear un entorno propicio para que Estados Unidos lidere en el ámbito de la IA y utilice su potencial para abordar desafíos sociales complejos. Se hace hincapié en la necesidad de invertir en educación, formación, investigación y desarrollo en IA, al tiempo que se abordan cuestiones de propiedad intelectual para proteger a los innovadores y creadores.

La Administración Biden, respaldará programas para dotar a los estadounidenses de las

[12] Es Importante destacar que este análisis no versa sobre el régimen jurídico de las órdenes ejecutivas en los Estados Unidos, sino en una extracción de valores y cuestiones de relevancia más general.

habilidades necesarias para la era de la IA y atraer talento mundial en este campo. Se promoverá un ecosistema y un mercado equitativos, abiertos y competitivos para la IA y tecnologías relacionadas, permitiendo que pequeños desarrolladores y emprendedores impulsen la innovación. Además, se buscará poner fin a la colusión ilegal y abordar los riesgos derivados del uso de activos clave por parte de empresas dominantes para perjudicar a competidores. Se apoyará un mercado que aproveche los beneficios de la IA para el avance y prosperidad de la sociedad.

En tercero lugar, se refleja que el desarrollo y uso responsables de la IA requieren un compromiso de apoyo a los trabajadores estadounidenses. Este objetivo destaca la importancia de garantizar que los trabajadores estadounidenses se beneficien del desarrollo y la implementación de la IA. Se reconoce que, si bien la IA puede crear nuevos empleos e industrias, es crucial que todos los trabajadores tengan un lugar en la mesa y puedan acceder a estas oportunidades. Se menciona específicamente la importancia de la negociación colectiva para asegurar que los trabajadores se beneficien de las oportunidades generadas por la IA. Además, se busca adaptar la formación y la educación laboral para apoyar una fuerza laboral diversa y facilitar el acceso a las oportunidades creadas por la IA.

En cuarto lugar, las políticas de Inteligencia Artificial se dice que tienen que ser coherentes con la dedicación de la Administración Biden a la promoción de la equidad y los derechos civiles. Este principio subraya la importancia de que las políticas relacionadas con la IA estén alineadas con el compromiso de la Administración Biden de promover la equidad y los derechos civiles. Se reconoce que los sistemas de IA desplegados de manera irresponsable pueden reproducir y amplificar las desigualdades existentes, así como causar nuevas formas de discriminación. La Administración se basará en iniciativas previas, como la publicación del Plan para una Declaración de Derechos de la IA, el Marco de Gestión de Riesgos de la IA y la Orden Ejecutiva 14091, para garantizar que la IA cumpla con todas las leyes federales y promueva evaluaciones técnicas sólidas, supervisión cuidadosa, participación de las comunidades afectadas y regulación rigurosa.

En quinto lugar, se deben protegerse los intereses de los estadounidenses que, cada vez más, utilizan, interactúan o compran IA y productos con IA en su vida cotidiana. Este objetivo

reconoce que el uso de nuevas tecnologías, como la IA, no exime a las organizaciones de sus responsabilidades legales, y que las protecciones al consumidor son fundamentales en momentos de cambio tecnológico.

El Gobierno Federal se compromete a hacer cumplir las leyes y principios existentes de protección al consumidor y a establecer salvaguardias adecuadas contra el fraude, los prejuicios involuntarios, la discriminación, las infracciones de privacidad y otros daños asociados con la IA. Se destaca la importancia de estas protecciones en áreas críticas como la salud, los servicios financieros, la educación, la vivienda, el derecho y el transporte.

En sexto lugar, se señala que la privacidad y las libertades civiles de los estadounidenses deben ser protegidas a medida que la IA sigue avanzando. Este principio destaca la importancia de proteger la privacidad y las libertades civiles de los estadounidenses a medida que avanza la inteligencia artificial, y hace un especial énfasis en la rapidez con la que esta avanza y se desarrolla. La IA está facilitando la extracción, reidentificación, vinculación, inferencia y acción sobre información sensible sobre la identidad, ubicación, hábitos y deseos de las personas. Las capacidades de la IA en estas áreas aumentan el riesgo de que los datos personales puedan ser explotados y expuestos.

Para combatir este riesgo, el Gobierno Federal garantizará que la recopilación, el uso y la retención de datos sean legales, seguros y mitiguen los riesgos de privacidad y confidencialidad. Las agencias[13] utilizarán herramientas políticas y técnicas disponibles, incluidas las tecnologías de protección de la privacidad (PETs) cuando corresponda, para proteger la privacidad y combatir los riesgos legales y sociales más amplios, incluida la inhibición de los derechos de la Primera Enmienda, que resultan de la recopilación y uso indebidos de los datos de las personas.

En séptimo y penúltimo lugar, se contempla la importancia de gestionar los riesgos del propio uso de la IA por parte del Gobierno Federal y aumentar su capacidad interna para regular, gobernar y respaldar el uso responsable de la IA para ofrecer mejores resultados

[13] El régimen jurídico de las Agencias Federales no es materia de este análisis, para más información acerca de las mismas consultar: https://www.usa.gov/agency-index

para los estadounidenses.

El Gobierno Federal se compromete a desarrollar y fortalecer sus capacidades internas para supervisar y regular el uso de la IA, garantizando que se utilice de manera responsable y ética en todas las áreas de su operación. Esto incluye la implementación de políticas, prácticas y procedimientos adecuados para mitigar los riesgos potenciales y garantizar que el uso de la IA esté alineado con los objetivos y valores del Gobierno y beneficie a la sociedad en su conjunto.

En octavo y último lugar, el Gobierno Federal debería liderar el camino hacia el progreso societal, económico y tecnológico global, como lo ha hecho Estados Unidos en eras anteriores de innovación disruptiva y cambio. Este liderazgo no se mide únicamente por los avances tecnológicos que EE. UU. ha logrado. Un liderazgo efectivo también implica ser pioneros en los sistemas y salvaguardias necesarios para desplegar la tecnología de manera responsable, y construir y promover esas salvaguardias con el resto del mundo.

La Administración Biden se comprometerá a colaborar con aliados y socios internacionales en el desarrollo de un marco para gestionar los riesgos de la IA, desbloquear su potencial para el bien y promover enfoques comunes para desafíos compartidos. Esto implica establecer una colaboración activa en el desarrollo de estándares y regulaciones internacionales que garanticen un despliegue seguro y ético de la IA en beneficio de toda la humanidad.

i. Aspectos más relevantes

Es importante resaltar que la técnica legislativa utilizada en las órdenes ejecutivas estadounidenses dificulta su lectura y comprensión[14][12], por lo que haremos un análisis de los asuntos de mayor interés relativos a la orden ejecutiva para tratar así de facilitar y agilizar la comprensión de los mismos dejando atrás la estructura formal propuesta en la propia orden.

[14] La ausencia de índice y estructura formal sistemática, además de su redacción en inglés con una terminología muy técnica complican el análisis concreto de los aspectos de la orden, por lo que nos centraremos nuevamente en los temas de mayor impacto y relevancia social.

a. La atracción de nuevo talento profesional

Estados Unidos busca la atracción de nuevos talentos en el campo de la inteligencia artificial, permitiendo la entrada y residencia en el país para los profesionales en la materia. El objetivo es fomentar la innovación y la competencia en este ámbito, agilizando el proceso de solicitud de visas y garantizando la disponibilidad de citas para no ciudadanos interesados en trabajar, estudiar o investigar en IA u otras tecnologías críticas y emergentes. EE. UU. tomará medidas para asegurar que haya suficientes citas disponibles para solicitantes con experiencia en estos campos, facilitando así su contribución al desarrollo económico y tecnológico de Estados Unidos.

Se establecerá, en la medida en que lo permita la ley y haya fondos disponibles, un programa para identificar y atraer talento destacado en inteligencia artificial y otras tecnologías críticas y emergentes en universidades, instituciones de investigación y el sector privado en el extranjero. Se establecerán y aumentarán las conexiones con ese talento para informarles sobre las oportunidades y recursos de investigación y empleo en los Estados Unidos, incluidos componentes educativos en el extranjero. Se proporcionará información sobre opciones de visas no inmigrantes e inmigrantes, así como la posible adjudicación acelerada de sus peticiones y solicitudes de visa.

Las autoridades competentes, en concordancia con la ley aplicable y las regulaciones de implementación, utilizarán sus facultades discrecionales para apoyar y atraer a ciudadanos extranjeros con habilidades especiales en inteligencia artificial y otras tecnologías críticas y emergentes que busquen trabajar, estudiar o realizar investigaciones en los Estados Unidos.

Además, se señala la elaboración de una guía clara y completa para los expertos en inteligencia artificial y otras tecnologías críticas y emergentes, con el fin de comprender sus opciones para trabajar en los Estados Unidos. Esta guía será publicada en varios idiomas relevantes en la web del Gobierno Federal[15]. Asimismo, se preparará un informe público que incluirá datos relevantes sobre solicitudes, peticiones, aprobaciones y otros indicadores

[15]Web oficial del Gobierno Federal de los Estados Unidos: https://ai.gov/

clave sobre cómo los expertos en inteligencia artificial y otras tecnologías críticas y emergentes han utilizado el sistema de inmigración hasta el final del año fiscal 2023.

b. Mejora y aumento de la infraestructura y medios

EE. UU. reconoce la gran importancia de la IA, y entiende que para poder desarrollarla correctamente es necesaria una alta inversión económica en el sector. Por ello, se establecerán al menos cuatro nuevos Institutos Nacionales de Investigación en Inteligencia Artificial[16], además de los 25 actualmente financiados en la fecha de esta orden.

Además, para apoyar actividades relacionadas con la informática de alto rendimiento y de gran intensidad de datos, se establecerá un programa piloto para mejorar los programas de formación existentes para científicos, con el objetivo de capacitar a 500 nuevos investigadores para el año 2025 capaces de satisfacer la creciente demanda de talento en inteligencia artificial.

Para garantizar el desarrollo y despliegue responsables de la inteligencia artificial en el sector educativo, se desarrollarán recursos, políticas y orientaciones sobre inteligencia artificial. Estos recursos abordarán los usos seguros, responsables y no discriminatorios de la inteligencia artificial en la educación, incluido el impacto de los sistemas de IA en comunidades vulnerables y desatendidas, y se desarrollarán en consulta con las partes interesadas según corresponda. También incluirán el desarrollo de un "conjunto de herramientas de IA" para líderes educativos que implementen recomendaciones del informe "IA y el Futuro de la Enseñanza y el Aprendizaje" del Departamento de Educación, incluyendo la revisión humana adecuada de decisiones de IA, el diseño de sistemas de IA para mejorar la confianza y seguridad y alinearse con las leyes y regulaciones relacionadas con la privacidad en el contexto educativo, y el desarrollo de barreras específicas para la educación.

Para incrementar la inversión de las agencias en inteligencia artificial, se priorizará la

[16] El término empleado es una aproximación al concepto europeo de Institutos Nacionales, para conocer la naturaleza jurídica con mayor precisión de estos institutos acudir: https://www.usa.gov/agency-index

financiación de proyectos de IA por un período mínimo de un año a través del Fondo de Modernización Tecnológica. Se insta a las agencias a presentar propuestas de financiamiento de proyectos a este fondo, fomentando así la modernización e inversión en el desarrollo e implementación de IA.

Todo esto refleja una complicación, y es que todas estas agencias y organismos tendrán que colaborar entre sí para poder lograr los objetivos planteados en la orden ejecutiva.

c. Make America Great Again

EE. UU. desde hace muchos años ha sido una gran potencia, y ha sido la precursora de multitud de nuevos avances, no solo a nivel tecnológico. Es por ello que la Administración Biden está intentado que esto vuelva a suceder ahora en materia de IA.

Por ello, para fortalecer el liderazgo de Estados Unidos en los esfuerzos globales para desbloquear el potencial de la inteligencia artificial y hacer frente a sus desafíos, EEUU liderará los esfuerzos para expandir los compromisos con aliados y socios internacionales en foros bilaterales, multilaterales y multipartidistas, promoviendo así la comprensión de las políticas de IA de Estados Unidos y mejorando la colaboración internacional.

Además, se contempla que EE. UU. se encargará de establecer un marco internacional sólido para gestionar los riesgos y aprovechar los beneficios de la IA, fomentando compromisos voluntarios similares a los realizados por empresas estadounidenses y coordinando actividades para desarrollar principios regulatorios y de responsabilidad comunes para naciones extranjeras. Para avanzar en los estándares técnicos globales responsables para el desarrollo y uso de IA, se trabajará de forma conjunta en la elaboración de un estándar de cooperación.

No obstante, la situación actual tampoco dista tanto de esta iniciativa estadounidense dado que, como se ha ido analizando hasta ahora y completaremos posteriormente con el análisis europeo, EE. UU. está jugando un rol de vital relevancia en el marco del desarrollo de la IA a nivel global.

Textos legislativos europeos

Hasta ahora, hemos centrado el análisis en los textos legislativos estadounidenses, pero ¿y Europa? A continuación, analizaremos los dos textos más importantes en el desarrollo del marco legislativo europeo en materia de IA, para concluir posteriormente con unas conclusiones orientadas a la comparativa entre ambos bloques.

Como ya mencionamos en la introducción de este trabajo, la IA y el tratamiento de los datos personales se encuentran íntegramente relacionados[17]. En el análisis relativo al *Artificial Intelligence Act (AIA)* observaremos que en el propio texto se menciona en múltiples ocasiones a RGPD, además, esta relación se lleva hasta el punto en el que habrá organismos propios de la protección de datos que jugarán roles esenciales en el tratamiento y regulación de estas inteligencias artificiales.

Hay que destacar que el análisis del AIA estará centrado en una visión global del texto, es decir, serán analizados los aspectos de mayor trascendencia para este análisis y obviaremos datos técnicos cuya relevancia práctica en este análisis no son esenciales.

a) Texto UE: *Artificial Intelligence Act*

Análisis general del contenido

La UE, consciente de la rápida evolución tecnológica y las posibles dificultades que puedan surgir, busca un enfoque equilibrado que preserve su liderazgo tecnológico y permita a los europeos beneficiarse de nuevas tecnologías, siempre en línea con los valores, derechos fundamentales y principios de la UE.

Es importante señalar que esta iniciativa legislativa responde al compromiso político de la presidenta Úrsula Von der Leyen, quien en sus orientaciones políticas para la Comisión 2019-2024[18] anunció la presentación de propuestas legislativas para abordar las

[17] Recordar la mención que hicimos acerca del art.22 RGPD y la sentencia SCHUFA del TJUE.
[18] https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_es_0.pdf

implicaciones éticas y humanas de la IA.

En este contexto, el 19 de febrero de 2020, la Comisión publicó el Libro Blanco[19] sobre la inteligencia artificial. Este Libro Blanco se contemplan dos objetivos primordiales: el promover la adopción de la IA y de abordar los riesgos vinculados a determinados usos de esta nueva tecnología.

Este texto legislativo se centra principalmente en el desarrollo normativo del segundo de estos objetivos: el abordar los riesgos derivados de la implementación de las inteligencias artificiales. Hay que destacar que se realiza el desarrollo sobre los valores y derechos fundamentales de la UE, que busca inspirar confianza en los ciudadanos y otros usuarios para adoptar soluciones basadas en la IA, al tiempo que fomenta a las empresas a desarrollar estas soluciones.

El Consejo Europeo, en sus Conclusiones de octubre de 2020[20], también destacó la necesidad de abordar la opacidad, complejidad, sesgo e imprevisibilidad de ciertos sistemas de IA, asegurando su compatibilidad con los derechos fundamentales y las normas jurídicas.

El Parlamento Europeo ha desempeñado un papel importante, aprobando resoluciones sobre ética, responsabilidad civil, derechos de propiedad intelectual y el uso de la IA en el ámbito penal, educativo, cultural y audiovisual[21].

En este contexto, la Comisión propone un marco reglamentario sobre IA con objetivos específicos:

- Garantizar que los sistemas de IA introducidos y utilizados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión.
- Asegurar la seguridad jurídica para fomentar la inversión e innovación en IA.

[19] Comisión Europea, Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final, 2020.
[20] Consejo de la Unión Europea, Conclusiones de la Presidencia - La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital, 11481/20, 2020.
[21] Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012(INL).

- Mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA.
- Facilitar el desarrollo de un mercado único para el uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.

Para lograr estos objetivos, la propuesta establece un enfoque normativo horizontal, equilibrado y proporcionado, que refleja una serie de requisitos mínimos para abordar los riesgos asociados con la IA sin obstaculizar el desarrollo tecnológico ni aumentar indebidamente el coste económico. El marco jurídico propuesto es sólido y flexible, con opciones reglamentarias amplias y un sistema regulatorio centrado en un enfoque basado en riesgos.

Es importante destacar que a lo largo del texto se contempla un interés particular acerca de que este texto normativo se mantenga en el tiempo, para ello emplea definiciones y objetivos no tan susceptibles a caer en el desfaso, algo que puede ocurrir muy fácilmente debido a la novedad de la materia a tratar.

No puede olvidarse que la propuesta debe ser coherente con la legislación de la Unión Europea vigente, especialmente en los sectores donde ya se utilizan o se prevé que se utilicen sistemas de IA de alto riesgo.

Esta coherencia se extiende a la Carta de los Derechos Fundamentales de la UE y al Derecho derivado de la Unión en áreas como la protección de datos, protección de los consumidores, no discriminación e igualdad de género.

Es importante destacar que la propuesta no afecta la aplicación del Reglamento General de Protección de Datos (RGPD) y la Directiva sobre protección de datos en el ámbito penal, sino que complementa estas regulaciones con normas armonizadas para el diseño, desarrollo y uso de sistemas de IA de alto riesgo, así como restricciones en ciertos usos de sistemas de identificación biométrica remota. Esto es muy importante, el propio texto normativo señala que actuará como complemento a la normativa vigente en materia de protección de datos, otro elemento más en relación de ambas materias.

Es preciso recordar que esta propuesta normativa constituye una parte integral de un conjunto más amplio de medidas destinadas a abordar los desafíos derivados del desarrollo y uso de la IA, tal como se analiza en el Libro Blanco sobre la inteligencia artificial.

Procede mencionar que el 19 de febrero de 2020, coincidiendo con la publicación del Libro Blanco sobre la inteligencia artificial, se inició una consulta pública en línea que se extendió hasta el 14 de junio de 2020. El propósito de esta consulta fue recabar observaciones y opiniones acerca del Libro Blanco. La convocatoria estuvo dirigida a todas las partes interesadas, tanto del sector público como del privado. Tras el análisis de todas las respuestas recibidas, la Comisión publicó un resumen de los resultados y las respuestas individuales en su sitio web[22].

En resumen, de estas respuestas individuales, las partes interesadas coinciden en la necesidad de tomar medidas. Una gran mayoría cree que existen lagunas legislativas o que se requiere una nueva legislación. Esto demuestra, además, el interés social en la creación de una legislación que regule la IA.

Hay que mencionar que durante la redacción del proyecto se hace continuas referencias a multitud de DDFF que se ven afectados por las IA y cómo serán tratados por la norma. Por tanto, la norma busca un alto nivel de protección para estos derechos fundamentales. Para lograr este objetivo, la propuesta impone ciertas restricciones a la libertad de empresa y a la libertad de las artes y las ciencias. Estas restricciones están destinadas a garantizar el respeto de los fines imperiosos de interés general relacionados con áreas como la salud, la seguridad, la protección de los consumidores y otros derechos fundamentales durante el desarrollo y uso de tecnologías de IA de alto riesgo. Sin embargo, algo fundamental es que estas restricciones se plantean de manera proporcionada y se limitan al mínimo necesario para prevenir y reducir riesgos graves para la seguridad y posibles violaciones de los derechos fundamentales.

[22] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0206

Análisis estructural

Debido a la división esquematizada y organizada que propone el AIA, seguiremos el orden de títulos planteados por el texto para llevar a cabo un breve análisis respecto a estos apartados. Hay que destacar que únicamente se centrará en análisis en el contenido de los títulos que susciten un mayor interés y se dejarán fuera de este análisis los demás.

En el primer título del AIA se delimita el alcance de las nuevas normativas que regulan la incorporación en el mercado, la implementación y el uso de sistemas de IA. Asimismo, se introducen las definiciones que regirán en todo el documento. A destacar, como es lógico, la definición de "sistema de IA" dada, que se ha concebido de forma neutral desde el punto de vista tecnológico, buscando perdurar en el tiempo ante la veloz evolución tanto tecnológica como del mercado en el ámbito de la IA[23].

En el Título II se presenta una lista de prácticas de IA prohibidas. El enfoque del AIA se basa en los riesgos, diferenciando entre usos de la IA que generan un riesgo inaceptable, alto o bajo/mínimo. La lista de prácticas prohibidas abarca todos los sistemas de IA cuyo uso se considera inaceptable por ser contrario a los valores de la Unión, como violar derechos fundamentales. Este título II plantea una clasificación de las distintas IA en base al tipo de riesgo que estas pueden generar, principalmente, en el individuo. Esto resalta el acentuado énfasis de las legislaciones occidentales en la protección del individuo[24]. Este título podría considerarse como el centro del análisis, dado que se trata de la primera clasificación concreta de los distintos riesgos que las IA pueden provocar en los individuos y, además, como veremos a continuación, bajo la amenaza de unas sanciones muy elevadas en caso de incumplimiento o quebrantamiento.

El Título III contiene normas específicas para los sistemas de IA que representan un alto riesgo para la salud, la seguridad o los derechos fundamentales de las personas físicas. No obstante, hay que destacar que estos sistemas de IA de alto riesgo sí pueden comercializarse

[23] Esta definición ya fue analizada en el apartado correspondiente a la definición del concepto de IA, por tanto simplemente haremos una breve mención a su ubicación en el texto normativo.
[24] Este tipo de cuestiones nos llevan a recordar el análisis previo realizado respecto a la protección de datos, centrado también en un análisis y regulación a partir del individuo como centro del problema.

en el mercado europeo, eso sí, siempre y cuando cumplan con los requisitos obligatorios y se sometan a una evaluación de conformidad previa.

Se definen dos categorías principales de sistemas de IA de alto riesgo: aquellos diseñados como componentes de seguridad de productos sujetos a una evaluación de conformidad previa, y otros sistemas independientes con implicaciones principalmente relacionadas con los derechos fundamentales.

El Capítulo 2 establece los requisitos legales que deben cumplir los sistemas de IA de alto riesgo en cuanto a datos y su gestión, documentación y registro, transparencia y comunicación de información a los usuarios, supervisión humana, solidez, precisión y seguridad. Estos requisitos mínimos propuestos se basan en directrices éticas para una IA confiable elaboradas por un grupo de expertos de alto nivel sobre IA, tras dos años de trabajo preparatorio. En definitiva, señala las pautas legales que deberán seguir estos sistemas considerados de alto riesgo.

Respecto a estos sistemas de IA de alto riesgo, se destaca que deberán ser diseñados y desarrollados de manera que garanticen un nivel suficiente de transparencia, permitiendo a los usuarios interpretar y utilizar adecuadamente la información que generan. Se asegurará que haya un tipo y nivel apropiados de transparencia para que tanto el usuario como el proveedor cumplan con las obligaciones establecidas. Por tanto, no solo se normativiza al proveedor, sino también al consumidor de estos sistemas.

Se contemplan algunas medidas destinadas a facilitar la transparencia y la utilización clara por parte de los usuarios de estos sistemas a través de tener que ir acompañados de instrucciones de uso correspondientes, presentadas en un formato digital u otro formato adecuado. Estas instrucciones contendrán información pertinente, accesible y comprensible para los usuarios, presentada de manera concisa, completa, correcta y clara.

Otra medida implementada en el AIA es que los sistemas de IA de alto riesgo serán diseñados y desarrollados de manera que puedan ser monitoreados de manera efectiva por personas físicas durante su uso, lo cual implica proporcionarles una herramienta de interfaz humano-máquina adecuada, entre otras medidas.

El propósito de esta vigilancia humana no es otro que el de prevenir o minimizar los riesgos para la salud, la seguridad o los derechos fundamentales que puedan surgir cuando un sistema de IA de alto riesgo se utilice de acuerdo con su propósito previsto o se le dé un uso indebido razonablemente previsible. Se señala, además, que esto será especialmente relevante cuando los riesgos persistan en el tiempo.

Ahora, fuera del título III y sin la necesidad de entrar en ningún otro título concreto dado que es una extracción de varios de ellos, se hace un desarrollo acerca de la creación de espacios controlados para probas las IA, donde los proveedores serán responsables de los daños causados en base a las normativas estatales que le sean de aplicación. No obstante, esto no es lo que más nos interesa, sino lo mencionado respecto a quién será uno de los encargados en regular estos espacios seguros. En efecto, será el Supervisor Europeo de Protección de Datos uno de los órganos competentes para su tratamiento. Esto, una vez más, señala la relación tan estrecha entre IA y datos personales, hasta el punto de ser un mismo órgano el encargado de supervisar ciertas acciones respecto a ambas materias.

Por otro lado, es relevante también la mención a la recomendación realizada por el propio Reglamento donde se insta a los distintos Estados miembro de la UE a crear códigos de conducta a nivel Estatal con el objetivo de facilitar el cumplimiento voluntario de las disposiciones contempladas en el Reglamento por parte de los sujetos afectados.

Para concluir con este desarrollo, destacada mención tiene el título X del Reglamento, destinado a las sanciones previstas para el caso de incumplimiento. Esto es, sin duda, lo más novedoso y llamativo de todo el texto, la contemplación de un marco sancionador estricto y concreto relativo a la utilización de la IA en base a los riesgos generados, que como mencionamos se clasifican en tres niveles distintos.

Las infracciones como el incumplimiento de la prohibición de prácticas de inteligencia artificial según el artículo 5[25] o de los requisitos del artículo 10 pueden resultar en multas administrativas de hasta 30 000 000 EUR o hasta el 6 % del volumen de negocio anual mundial del ejercicio financiero anterior para empresas, si esta última cifra es mayor.

[25] Para ver el art.5 y 10, acudir al propio AIA: https://lc.cx/tdeYh8

Además, el incumplimiento de cualquier requisito u obligación establecido en el Reglamento, excepto los de los artículos 5 y 10, puede acarrear multas de hasta 20 000 000 EUR o hasta el 4 % del volumen de negocio anual mundial del ejercicio financiero anterior para empresas, si esta última cifra es mayor.

Conclusiones respecto al análisis del AIA

En definitiva, podemos observar cómo el AIA muestra de una manera muy ordenada y precisa cuál es el concepto de la IA y destinado a perdurar en el tiempo, su impacto respecto al individuo, un análisis de este impacto en base a una clasificación del riesgo que las mismas pueden ser capaces de producir, una serie de métodos para propiciar un cumplimiento del Reglamento de manera voluntaria por los distintos sujetos afectados y, por último, un régimen sancionador considerable para los casos de incumplimiento.

Debemos destacar que, pese a la notoria diferencia de claridad respecto a los objetivos de los textos estadounidenses y el AIA, muchos aspectos tratados en los distintos textos se tratan de puntos de convergencia. Esto lo analizaremos posteriormente de manera más detallada en un apartado específico del análisis.

Este análisis permite la observancia respecto a un texto sólido y con proyección próxima a ser adoptado. No podemos obviar el dato de que esta normativa, cuya perspectiva es adoptar fuerza de Reglamento, será de aplicación directa en el seno del marco legislativo de los veintisiete Estados miembros de la UE. Esto se trata de todo un hito normativo. Esto es debido a que conseguir una regulación tan minuciosa en una materia tan poco explorada y con tantos sujetos tan diferentes entre sí suscita una complejidad absoluta.

b) Texto CdE: *Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law*

Hasta ahora, el análisis que hemos llevado a cabo de los anteriores textos normativos ha sido siguiendo un esquema bastante concreto, dado que el contenido de estos textos era muy amplio y divergente entre sí. No obstante, el texto planteado por parte del CdE busca un objetivo diferente a los anteriores. Este texto busca la convergencia en el marco

internacional respecto a la aplicación y regulación de la IA.

Es por ello, que el análisis de este texto normativo no será realizado tan sistemáticamente sino más bien señalando los aspectos fundamentales del mismo. Esto es así debido a que este texto, y adelantamos por completo las conclusiones del trabajo, va a actuar como marco legislativo de convergencia total entre el bloque de los EE. UU. y la UE, siendo esta la tesis defendida en este trabajo.

Esto es hasta el punto de que los EE. UU., como todo aparenta, será un firmante de este tratado internacional, por tanto, quedará vinculado de igual manera que los Estados firmantes de la UE.

Hasta ahora, siempre hemos hablado de aspectos de uno u otro bloque, pero aquí nos centraremos en este marco que aparentemente ambos asumirán como base de su desarrollo normativo.

Análisis del contenido: punto de convergencia normativo

Para comenzar, el texto hace referencia a una premisa defendida desde un inicio tanto por el bloque normativo estadounidense como europeo: la afirmación de que la IA en sí misma proporciona multitud de ventajas y beneficios, pero que también genera riesgos que tienen que ser objeto de análisis. Se contempla, además, la forma de llevar a cabo este análisis: a través de la información extraída por medio de la experiencia de los riesgos que supone la IA en sus distintas formas.

Se acentúa, además, que en el ámbito de la IA el uso indebido puede provocar consecuencias muy perjudiciales para el individuo, que recordemos en ambos sistemas actuaba como centro del problema y manteniéndose este principio también aquí.

Por otro lado, en su preámbulo, el texto afirma claramente cuál es su objetivo, como se ha mencionado anteriormente: la creación de un marco legal común estableciendo principios y reglas en relación con el ciclo de vida de la IA con el fin de hacer prevalecer los aspectos comunes y ensalzar los beneficios de la IA sobre los perjuicios que puede suponer.

Es necesario destacar que en el preámbulo se señalan multitud de instrumentos de defensa de los derechos humanos, los cuales estarán perfectamente respetados por el contenido y aplicación de esta norma. Inspirados todos ellos por la Declaración Universal de Derechos Humanos, de 1948.

Existe la necesidad, no obstante, debido a la generalidad del texto, de que los Estados firmantes del tratado internacional creen normativa nacional dirigida a la correcta implementación y aplicación del contenido reflejado en este tratado.

Por supuesto, en el art.2 del tratado se contempla una definición de IA[26]. Esto implica que pese a las divergencias que se han podido ir matizando durante el análisis, estas quedarán corregidas y alineadas con el concepto aquí proporcionado.

A lo largo del texto se señalan aspectos que sí han sido señalados previamente en algunos de los textos analizados, pero no en todos, como puede ser la exigencia de la creación de espacios seguros para el desarrollo de IA, o la necesidad de garantizar la transparencia e informar al individuo cuando esté bajo el tratamiento de una IA.

Se señala, por otro lado, que los firmantes deberán, más allá de cumplir todo lo previamente mencionado, servir de apoyo para otros Estados no firmantes para la actuación conforme a los principios y directrices planteadas en este texto. Además, las partes firmantes deberán compartir información relativa a la IA, en todos sus ámbitos, con los demás Estados firmantes para poder ir creando una cohesión entre todos ellos.

Aunque no se establezca un régimen sancionador, sí se establece un régimen cautelar. En los artículos 14 y 15 se establecen disposiciones para garantizar la protección de los derechos humanos en el contexto de los sistemas de inteligencia artificial (IA). El artículo 14 enfatiza la necesidad de adoptar medidas para proporcionar remedios accesibles y efectivos en caso de violaciones de derechos humanos relacionadas con la IA. Esto incluye

[26] Art. 2 CAI "A efectos del presente Convenio, se entenderá por "sistema de inteligencia artificial" un sistema basado en una máquina que, con objetivos explícitos o implícitos, infiere, a partir de los datos de entrada que recibe, cómo generar como predicciones, contenidos, recomendaciones o decisiones que puedan influir en entornos físicos o virtuales. Los distintos sistemas de inteligencia artificial varían en sus niveles de autonomía y adaptabilidad tras su despliegue".

la documentación y divulgación de información relevante sobre los sistemas de IA, así como la posibilidad de que las personas afectadas impugnen decisiones y presenten quejas ante las autoridades competentes. Por otro lado, el artículo 15 destaca la importancia de garantizar garantías procesales efectivas cuando los sistemas de IA tienen un impacto significativo en los derechos humanos, y aboga por la notificación adecuada a las personas que interactúan con estos sistemas en lugar de con seres humanos. Estas disposiciones buscan establecer un marco jurídico sólido para proteger los derechos de las personas en un entorno cada vez más influenciado por la IA.

En concordancia con lo anterior se establece que cada parte firmante debe adoptar medidas para identificar, evaluar, prevenir y mitigar los riesgos asociados con los sistemas de inteligencia artificial (IA), considerando su impacto en los derechos humanos, la democracia y el estado de derecho. Estas medidas deben ser graduadas y diferenciadas, teniendo en cuenta el contexto y el uso previsto de los sistemas de IA, la gravedad y probabilidad de los impactos, las perspectivas de las partes interesadas relevantes, y deben aplicarse de manera iterativa a lo largo del ciclo de vida de los sistemas de IA. Además, se requiere documentar los riesgos y los impactos, y se debe realizar pruebas antes de implementar nuevos sistemas de IA o realizar modificaciones significativas. Se deben adoptar medidas para abordar adecuadamente los impactos negativos en los derechos humanos, la democracia y el estado de derecho, y se debe evaluar la necesidad de prohibir ciertos usos de los sistemas de IA si se considera que son incompatibles con el respeto a los derechos humanos, la democracia o el estado de derecho. Esto, podría decirse que ya realmente ya lo están llevando a cabo ambos bloques.

Para concluir, se menciona que la firma de este tratado internacional no supondrá la exclusión de acuerdos previamente realizados en materia de IA por los firmantes, sino que será perfectamente compatible con todos ellos salvo en los casos donde el objeto de este tratado no sea respetado o incompatible con el otro.

Conclusiones

Respecto al análisis de los datos personales hemos podido esclarecer que, pese a la enorme

diferencia de tendencias existente en el globo respecto al concepto y la rigidez con la que regular los datos personales, en los Estados de mayor impacto en el mundo sí están siendo regulados estos datos personales. Es decir, los Estados continúan legislando y adaptando las normativas en materia de protección de datos a la realidad actual.

La diferencia más acentuada e interesante se encuentra, no obstante, en el propio concepto, donde muchos de los Estados ni siquiera tratan el dato "personal", sino más bien aspectos comerciales o sanitarios relativos a datos que circulan. Por lo general, se puede afirmar que muchos Estados son muy reacios al aspecto "personal". Esto, de manera muy resumida, se debe a que un reconocimiento del aspecto "dato personal" dentro de los textos fundamentales de estos respectivos Estados implicaría una obligación estatal de defenderlo, algo muy complejo y realmente costoso. Por último, quedó más que señalada la relación casi de dependencia entre la IA y los datos, donde sirven de base para el funcionamiento de la IA.

Continuamos nuestro análisis respecto a cuatro textos normativos, relativos a dos bloques occidentales distintos: EE. UU. y Europa. Se expuso cómo el *blueprint* remarcó una serie de principios considerados fundamentales, incluso fuera de EE. UU., para el desarrollo normativo de la IA; por otro lado, se explicaron estos cinco principios en un marco de aplicación más práctico dentro de la e*xecutive order*. Todo esto nos presentó un panorama cautelar respecto a la regulación normativa. Un panorama lleno de principios, objetivos e ideas, pero carente de sanciones de gran magnitud relativas al daño que pudiese ser provocado por estos sistemas de IA a los individuos.

EE. UU. refleja un enorme interés en estas nuevas tecnologías, queriendo utilizarlas como un nuevo marco de atracción de talento, facilitando los arduos trámites de visado a los interesados para poder acceder y residir dentro del país. Por otro lado, tenemos la legislación europea. Una legislación, en el marco de la UE, mucho más desarrollada que la estadounidense, donde sí se contempla un análisis del riesgo en tres grupos diferenciados con un régimen sancionador destacable.

La Unión Europea ha logrado formular un reglamento mucho más detallado que será de aplicación directa en el territorio de los 27 Estados miembros. Esto sería el mayor hito hasta

la fecha en materia legislativa de IA, dado que se dejarían atrás las diferencias conceptuales y normativas que tanto hemos observado a lo largo del análisis y, además, se conseguiría una unidad en una gran parte del territorio mundial.

Respecto a ambos bloques normativos también podemos encontrar similitudes, y debemos partir de la más fundamental de todas: no se regulan inteligencias artificiales, sino los riesgos que su utilización puedan llegar a provocar.

Esto es fundamental, y se debe a que todos los Estados parte de la premisa de que las nuevas tecnologías, su proliferación, como mencionábamos al inicio de la exposición, no puede detenerse. Una regulación de inteligencias artificiales concretas sería una norma condenada al colapso de manera muy rápida, debido a esta proliferación.

Por otro lado, ambos bloques parten de otra segunda premisa fundamental, la defensa del individuo como parte central del problema. Todas las iniciativas, principios y normas que hemos mencionado están centradas en defender al individuo frente al alcance e impacto que estas IA pueden producir en sus vidas diarias. Es decir, se busca el avance tecnológico en todo caso, pero controlado y protegiendo al individuo respecto a los daños que esta puede llegar a provocar sobre él.

Por último, el CdE. propone algo que era completamente necesario en el marco internacional, un punto de convergencia de todas estas visiones tan distintas entre sí. Cada Estado, como es sabido, tiene soberanía para poder dictar normas en su territorio, pero también es sabido que un Estado aislado por completo del régimen internacional está condenado al colapso y su marginación. Vivir al margen de la realidad internacional es muy complicado, y es por ello que las relaciones internacionales son fundamentales para los Estados.

Esto es de aplicación directa en el ámbito de la IA, donde por muchas ideas individuales que puedan tener los distintos bloques normativos a lo largo del mundo, siempre es necesario observar fuera de nuestras propias fronteras y tomar iniciativas e ideas en base a la observancia.

Esto es, precisamente, lo que el CdE busca: un punto donde los distintos bloques

internacionales puedan adherirse y compartir información y visiones entre ellos para después poder legislar de manera eficaz en el ámbito de la legislación nacional.

Por todo ello, el CdE propone un texto más orientado, bajo mi punto de vista, a la tendencia estadounidense. Esto lo baso en que la UE sí ha entrado a legislar de manera estricta el ámbito de la IA, mientras que el CdE y EE. UU. han optado más bien por un marco de principios y mínimos para posteriormente regular en consecuencia. Recordemos, que el Convenio propuesto por el CdE está pendiente de votación final[27] y, si todo transcurre como aparenta, sí será firmado por EE. UU. y los Estados miembros de la UE. Esto implicará el establecimiento del Convenio del CdE como punto de referencia internacional y posteriormente la UE y EE. UU., por su lado, regularán en materia, pero siempre respetando estos mínimos.

En definitiva, este análisis nos lleva a la idea final de que, pese a la complejidad de la materia y las enormes travas existentes para su entendimiento y regulación, la cooperación entre países unidos en torno a los valores humanos fundamentales termina por hacer posible la adopción de un consenso internacional.

Bibliografía

Act on the Protection of Personal Information (APPI), 2003.

Agencia Española de Protección de Datos. (s.f.). https://www.aepd.es/

Artificial Intelligence Act. (s.f.). Resumen de alto nivel. https://artificialintelligenceact.eu/es/high-level-summary/

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies.* W. W. Norton & Company.

Bundesdatenschutzgesetz [Federal Data Protection Act], 30 de junio de 2017 (Federal Law Gazette I p. 2097).

California Consumer Privacy Act (CCPA), 2018.

Council of Europe. (1985). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

[27] Nota final: el CAI ha sido aprobado hoy 17/05/2024 en Consejo de ministros, y estará disponible para su firma por los Estados interesados a partir de septiembre de este mismo año.

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law [Vilnius, 5.IX.2024]. Aprobado el 17 de mayo de 2024 por el Consejo de ministros.

EDPB (European Data Protection Board). (2021). Guidelines on the Interplay between the Second Payment Services Directive and the GDPR. EDPB.

Encuentro Iberoamericano de Protección de Datos (EIPD), La Antigua, Guatemala, 1- 6 de junio de 2003.

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021) 206 final, 2021/0106 COD).

European Union Agency for Fundamental Rights. (2018). Big Data, Artificial Intelligence and Privacy. https://fra.europa.eu/en

Executive Order No. 14110, 3 C.F.R. 789 (2023). Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

Frey, C. B., & Osborne, M. A. (2013). *The future of employment: How susceptible are jobs to computerization?* University of Oxford.

Hine, E., & Floridi, L. (2023, 29 de enero). The Blueprint for an AI Bill of Rights: In search of enaction, at risk of inaction.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018.

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (Francia).

Personal Data Protection Act (PDPA), 2012. Personal Information Protection Law (PIPL), 2021. Personal Protection Information Act (PIPA), 2011.

Red Iberoamericana de Protección de Datos. (2017). Estándares de protección de datos personales para los Estados Iberoamericanos.

Topol, E. (2019). Deep medicine: How artificial intelligence can make healthcare human again. Basic Books.

White House Office of Science and Technology Policy. (2022). The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American *People.*