APM 3.9.

Publicación digital. - Asociación Profesional de la Magistratura

ALFONSO PERALTA GUTIÉRREZ

ANDALUCÍA ORIENTAL

LA ESTRECHA CONEXIÓN ENTRE LA INTELIGENCIA ARTIFICIAL Y LA PRIVACIDAD

1. INTRODUCCIÓN

La inteligencia artificial (IA) ha emergido como una de las tecnologías disruptivas más fascinantes y prometedores en las últimas décadas en lo que se denomina la Cuarta Revolución Industrial. Con una velocidad mucho mayor de la que se esperaba en los últimos años, fruto principalmente de un avance exponencial producido durante la pandemia COVID, la IA ha comenzado a transformar prácticamente todos los aspectos de nuestra sociedad, desde la atención médica hasta la educación, la cultura y el arte, pasando por la seguridad, negocios o la industria manufacturera, hasta la conducción autónoma y la asistencia personalizada, incluyendo por supuesto el ámbito jurídico, la administración de Justicia e incluso la función jurisdiccional. Y fruto de ello, ha surgido un debate con noticias constantes en los que

no hay día que no surja una última hora sobre usos, riesgos, o declaraciones de expertos sobre esta tecnología emergente.

La Inteligencia Artificial se alimenta de un conjunto enorme de datos (*big data)* y de información, compuesta de textos, imágenes, vídeos, audios, datos de usuario, metadatos, datos del comportamiento, hábitos, datos biométricos y cualesquiera otros tipos de datos, como los especialmente sensibles como los médicos. Los datos son el petróleo del siglo XXI. Pero la IA no siempre tiene el conocimiento para comprender toda esa información y evaluarla conforme a su contexto, y mucho menos la sabiduría para interpretarla y aplicarla a su contexto, e incluso a problemas distintos.

Sabemos las estimaciones de lo que va a suponer la Inteligencia Artificial a la economía, los beneficios de una próxima era de las máquinas, su afectación transversal a todos los sectores, pero también sus riesgos como la opacidad ("la caja negra"), los sesgos, imprevisibilidad, o fallos de eficacia, así como la posibilidad de ser utilizada indebidamente y proporcionar herramientas novedosas y potentes para prácticas de manipulación[1], explotación y control social que pueden repercutir negativamente en derechos fundamentales como la igualdad y no discriminación, dignidad humana, privacidad, libertad de expresión y de información, presunción de inocencia, derecho a un juez imparcial y la propia democracia en sí misma.

Dado el gran impacto que la inteligencia artificial puede tener en la sociedad y la necesidad de generar confianza, es vital que la inteligencia artificial y su marco regulador se desarrollen de acuerdo con la Carta de los Derechos Fundamentales de la UE y los valores en los que se basa la Unión.

Por ello, la IA ha de considerarse una herramienta, y como cualquier herramienta podrá utilizarse para hacer el bien o el mal, lo que hay es que regular los malos usos, sus prohibiciones, y castigarlos. La Inteligencia Artificial ha venido para quedarse y nos va a afectar en casi todo nuestro entorno. Al contrario que la famosa carta de expertos que pide paralizar la IA, la inteligencia artificial no se trata ni de un genio que puedas volver a meter en la botella o de un expediente que puedas esconder en un cajón.

Para ello, surge el Reglamento Europeo de Inteligencia Artificial (*AI Act[2])*, cuyo objetivo es promover la adopción de la inteligencia artificial centrada en el ser humano y fiable y garantizar un alto nivel de protección de la salud, la seguridad, los derechos fundamentales, la democracia y el Estado de Derecho y el medio ambiente, frente a los efectos nocivos de los sistemas de inteligencia artificial en la Unión, apoyando al mismo tiempo la innovación y mejorando el funcionamiento del mercado interior. Y es que, las tecnologías disruptivas, como las basadas en componentes IA, deben también implementar las garantías de calidad y seguridad suficientes, sin que su novedad sea excusa de su cumplimiento.

Dado que la inteligencia artificial se basa a menudo en el tratamiento de datos personales, la normativa de protección de datos, sus autoridades de control, sus organismos consultivos, sus estándares de calidad, servicios de auditoría, evaluaciones de impacto y sistemas de análisis de riesgos, así como la implementación de delegados de protección de datos (*DPO, Data Protection Officer*) en las estructuras en las organizaciones sientan las bases para un régimen jurídico proporcionado y eficaz de normas vinculantes para los sistemas de IA, enfocado claramente en los usos de riesgo de la inteligencia artificial.

En los últimos tiempos, puede que fruto de la moda por la IA, o por la decisión de la creación de la Agencia de Supervisión de la Inteligencia Artificial (AESIA) separada de la AEPD, o la Oficina Europea de IA (EAI

---

[1] Europol. (2023). ChatGPT. The impact of Large Language Models on Law Enforcement. Tech Watch Flash. 27 de marzo de 2023. Consultado 1 de agosto de 2023. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

[2] Parlamento Europeo. (2023). Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD). Consultado el 25 de junio de 2023. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.html

Office), los Coordinadores de Servicios Digitales y su Junta Europea de Coordinación, separada del European Data Protection Supervisor, al igual que el European Data Protection Board, el Foro Consultivo de IA (AI Advisory Forum) o el Centro Europeo de Transparencia Algorítmica (ECAT) y los sandbox, todos ellos separados entre sí. O puede que porque el debate académico sobre la IA ha estado alejado de las prácticas diarias de auditoría y gestión de riesgos, o el que la IA está liderada por ingenieros y la protección de datos por juristas, e incluso una posible desgana del mundo de la privacidad hacia la inteligencia artificial ha podido parecer que la inteligencia artificial y la protección de datos no tienen tanto que ver. Recuerdo que hubo muchas personas a las que le sorprendió que el Garante italiano para la Protección de Datos Personales bloqueara ChatGPT[3] requiriendo una serie de medidas: ¿Cómo algo tan aburrido como la privacidad podía detener algo tan moderno y rupturista como la IA?

Sin embargo, la IA y la protección de datos tienen una estrecha conexión.

2. PRINCIPIOS DE PROTECCIÓN DE DATOS APLICABLES A LA INTELIGENCIA ARTIFICIAL.

Como hemos dicho, el entrenamiento de los sistemas de machine learning requiere grandes cantidades de datos para aprender y extraer el valor de esos grandes conjuntos de datos.

Los datos personales son, en muchos casos, una premisa clave para las decisiones autónomas. Y la "gobernanza de la privacidad y los datos" significa que los sistemas de IA se desarrollarán y utilizarán de conformidad con las normas vigentes sobre privacidad y protección de datos, procesando al mismo tiempo datos que cumplan normas estrictas de calidad e integridad.

Por lo tanto, el cumplimiento normativo de la IA Act irá de la mano del RGPD[4] y LOPDGDD[5] y únicamente, en caso de ausencia de datos personales, este tratamiento no estará sujeto al RGPD sino únicamente al AI Act en caso de sectores de alto riesgo. Pero para ello, habrá que demostrar que la eliminación o anonimización de los datos personales es realmente efectiva y evaluar cuál es el posible riesgo de reidentificación que existe.

A. Base de legitimación.

Desde el punto de vista de la Protección de Datos, la base de legitimación es el primer elemento que hay que establecer dentro de la fase de concepción del tratamiento. Si no se encuentra una base legitimadora no se debe realizar el tratamiento. Así, el regulador italiano exigió a ChatGPT cambiar la base legal del procesamiento de los datos personales de los usuarios con fines de entrenamiento algorítmico, eliminando cualquier referencia al contrato y asumiendo como base legal del procesamiento el consentimiento o interés legítimo en relación con las evaluaciones de competencia de la empresa en una lógica de responsabilidad. Es decir, el interés legítimo se supedita a una ponderación de la necesidad, idoneidad y proporcionalidad, de acuerdo a su fuente, naturaleza, impacto y garantías con los intereses o

[3] Garante privacy. (2023). ChatGPT: Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. Roma, 12 de abril de 2023. Consultado 1 de agosto de 2023. Disponible en https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751

[4] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) LA LEY 6637/2016.

[5] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales LA LEY 19303/2018.

los derechos fundamentales de los usuarios. Tampoco puede un responsable arrogarse razones, por ejemplo, de interés público si no está establecido en una norma del rango apropiado.

Sin embargo, en ocasiones este tipo de sistemas se entrenan con una gran cantidad de datos similar a "pesca de arrastre" que captura todo lo que va encontrando de una manera no selectiva a través de herramientas de web scraping. Al parecer ya se habrían interpuesto las primeras demandas contra el revolucionario sistema **ChatGPT** de OpenAI. La primera[6] se basaría en la vulneración de datos personales, en cuanto que el sistema habría "escrapeado" datos personales de manera no autorizada y en ocasiones el propio sistema "alucina", por lo que los principios de veracidad, exactitud, calidad, y transparencia de los datos se verían puestos en cuestión. Y es que lo cierto es que no sabemos de qué datos se ha alimentado ChatGPT. Lo poco que sabemos es por una investigación del Washington Post[7]. Musk[8] ha amenazado con demandarles porque cree que le han escrapeado Twitter. Esos sesgos, discriminaciones o polarizaciones que a veces vemos en ChatGPT4 tendría sentido que vinieran de redes sociales y no de publicaciones de medios de comunicación, patentes, o Wikipedia. Parece el mismo patrón. En este sentido, el servicio de Bing de Microsoft con GPT4 con la citación de fuentes es claramente una evolución y una buena práctica.

La segunda demanda contra ChatGPT[9] habría sido por presunta vulneración de derechos de autor. Y la razón es bastante simple, si Chatgpt no se ha alimentado de obras con derechos de autor, ¿cómo puede hacer resúmenes de libros con copyright? ¿Y cómo puede hacer resúmenes de libros de los que se supone que no tiene su contenido? Sin que realice referencias o cite la fuente, y no se pueda saber si saca un resumen de otros resúmenes o un resumen de la fuente original, resulta difícil responder la cuestión. New York Times[10] podría solicitar que un juez federal ordene a OpenAI que destruya el conjunto de datos de ChatGPT que haya sido entrenado con su contenido ilegalmente y vuelva a recrearlo usando solo datos que estén autorizados y abonar además cuantiosas multas.

De igual manera otros sistemas de IA generativa como Bard[11], Llama[12], NeoCortext[13], Stability AI[14] o Prisma

---

[6] THORBECKE, Catherine. (2023). OpenAI, maker of ChatGPT, hit with proposed class action lawsuit alleging it stole people's data. CNN. 28 de junio de 2023. Consultado el 1 de julio de 2023. Disponible en: https://edition.cnn.com/2023/06/28/tech/openai-chatgpt-microsoft-data-sued/index.html

[7] Schaul, K., Chen, S. Y., & Tiku, N. (2023). Inside the secret list of websites that make AI like ChatGPT sound smart. The Washington Post. 19 de abril de 2023. Consultado el 1 de agosto de 2023. Disponible en: https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/

[8] MEYER, David. (2023). 'Lawsuit time': Elon Musk explodes after Microsoft's Twitter ad snub. Fortune. 20 de abril de 2023. Consultado el 1 de agosto de 2023. Disponible en: https://fortune.com/2023/04/20/lawsuit-time-elon-musk-explodes-after-microsofts-twitter-ad-snub/amp/

[9] Brittain, Blake. (2023). Lawsuit says OpenAI violated US authors' copyrights to train AI chatbot. Reuters. 29 de junio de 2023. Consultado el 1 de julio de 2023. Disponible en: https://www.reuters.com/legal/lawsuit-says-openai-violated-us-authors-copyrights-train-ai-chatbot-2023-06-29/

[10] ALLYN, Bobby. (2023). 'New York Times' considers legal action against OpenAI as copyright tensions swirl. NPR. 16 de agosto de 2023. Consultado el 18 de agosto de 2023. Disponible en: https://www.npr.org/2023/08/16/1194202562/new-york-times-considers-legal-action-against-openai-as-copyright-tensions-swirl

[11] THE FASHION LAW. (2023) Google Angling for Dismissal in AI Lawsuit Accusing it of "Stealing" Data. 19 Octubre 2023. Consultado el 1 de julio de 2023. Disponible en: Google Angling for Dismissal in AI Suit Accusing it of Stealing Data (thefashionlaw.com)

[12] Thaler, S. (2023, Julio 10). Comedian Sarah Silverman sues OpenAI and Meta over copyright infringement. New York Post. Consultado el 1 de julio de 2023. Disponible en: Sarah Silverman sues OpenAI and Meta for copyright infringement (nypost.com)

[13] KYLAND YOUNG v. NEOCORTEXT INC (2023) United States District Court, C.D. California. Case No. 2:23-cv-02496-WLH(PVCx) Decided: September 05, 2023. Consultado 22 octubre de 2023. Disponible en: KYLAND YOUNG v. NEOCORTEXT INC (2023) | FindLaw

[14]THE FASHION LAW. (2023). "Stability AI Seeks Dismissal of Getty's Generative AI Copyright & TM Lawsuit." (2023) The Fashion Law. Consultado 22 octubre de 2023. Disponible en:

Labs[15] han sido demandados. En general, al igual que la aplicación de OpenAI se les acusa de vulnerar protección de datos o propiedad intelectual.

Otro caso bien conocido de raspado web es el de la empresa ***Clearview. AI,*** un motor de búsqueda de reconocimiento facial con una base de datos que afirman de más de 10 mil millones de imágenes faciales que mediante técnicas de web scraping, han sido extraídas de redes sociales (por ejemplo, Twitter o Facebook), blogs, medios de comunicación, webs de fichas policiales y, en general, de sitios web como vídeos de Youtube, las procesa algorítmicamente con técnicas biométricas para determinar su coincidencia y cuando un cliente consulta la base de datos y envía una imagen para buscar, se compara con las recopiladas.

Tras sucesivos expedientes y multas millonarias por autoridades de protección de datos de medio mundo, a nivel judicial lo más importante sería el acuerdo[16] al que esta empresa habría llegado ante el juez Sharon Johnson Coleman del Juzgado de Distrito Norte de Illinois para evitar una demanda colectiva por vulneración de protección de datos en Estados Unidos por una cantidad millonaria que ni siquiera se habría hecho pública.

En palabras de ESTEBAN RUIZ[17], el nivel de protección de datos, el mero «acceso» a datos personales entra dentro del ámbito de aplicación de la normativa de protección de datos y debe cumplir con las obligaciones ahí establecidas. Y ello, aunque esta información provenga de fuentes de acceso público o fuentes accesibles al público. Por lo tanto, el que los datos se encuentren accesibles al público no supone que no se aplique la normativa de protección de datos ya que existe un tratamiento de datos personales.

La AEPD[18] entiende con la presentación de un Código de Conducta del sector infomediario, presentado por la Asociación Multisectorial de la Información (ASEDIE) y publicado el pasado abril de 2021 que no existe un término legal de «fuente accesible al público» y que, por tanto, no existe un interés legítimo automático y general para usar los datos que provengan de estas fuentes. El uso de estas fuentes, por tanto, deberá estar sujeto a los principios de la normativa de protección de datos, incluyendo la necesidad de tener una base jurídica y la obligatoriedad de dar información al usuario sobre el tratamiento de sus datos personales en los términos previstos en RGPD. Y es que se trata del principio de limitación del tratamiento, por el cual una base jurídica no habilita para el uso de los datos para cualquier propósito y en todo momento.

Así, ese scraping de datos personales podría vulnerar la normativa de protección de datos. Asimismo, en dicho tratamiento de datos en virtud del principio de transparencia previsto en el art. 5.1.a) del RGPD no se habría dado, por ejemplo, información a las personas cuyos datos han sido recolectados al respecto sobre el tratamiento que va a realizarse (algo que debería comunicarse en el plazo de un mes desde el acceso a los datos), ni han prestado otra base de legitimación, lo que está íntimamente relacionado con el principio de información y transparencia.

---

https://www.thefashionlaw.com/stability-ai-seeks-dismissal-of-gettys-generative-ai-copyright-tm-lawsuit/

[15] THE FASHION LAW. (2023). "AI Avatar Generator Lensa Lands on Receiving End of Biometric Data Lawsuit." The Fashion Law. Consultado 22 octubre de 2023. Disponible en: https://www.thefashionlaw.com/ai-avatar-generator-lensa-lands-on-receiving-end-of-biometric-data-lawsuit/

[16] DAVIS, Wendy. (2023). Facial-recognition company Clearview settles Privacy Class-action. Mediapost. 22 de septiembre de 2023. Consultado el 22 de septiembre de 2023. Disponible en: https://www.mediapost.com/publications/article/389525/facial-recognition-company-clearview-settles-priva.html

[17] ESTEBAN RUIZ, Adaya María. (2022, 21 de noviembre). Entrenamiento de redes neuronales con datos de fuentes públicas, web scrapping y el problema de la falta de transparencia y trazabilidad de la información (1). Diario La Ley.

[18] Informe de la Agencia Española de Protección de Datos número 0089/2020. (2020). Consultado el 29 de enero de 2023. Disponible en: https://www.aepd.es/es/documento/2020-0089.pdf

B. **Proporcionalidad**

El RGPD exige que el tratamiento de los datos personales sea proporcional a su finalidad. Esto es, la minimización de los datos, que se define implícitamente en el artículo 5.1.c del reglamento, como el proceso dirigido a garantizar que los datos personales son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Y es esencial garantizar este tipo de principios de la privacidad desde el diseño y por defecto en todo el ciclo de vida de la IA como parte de un enfoque global de "ética desde el diseño".

C. Transparencia.

Estas tecnologías, independientemente del ámbito en el que se desarrollen, desplieguen y utilicen, deben ser desarrolladas desde el diseño de manera segura, rastreable, técnicamente sólida, fiable, ética y jurídicamente vinculante y ser objeto de un control y una supervisión independientes. Y para ello resultan esenciales las condiciones de explicabilidad, auditabilidad, trazabilidad y transparencia en cuanto que no siempre es posible explicar por qué un modelo ha dado lugar a un resultado o una decisión en concreto, como por ejemplo en el caso de los algoritmos de «caja negra». Así, el respeto de estos principios es condición necesaria para poder asegurar la rendición de cuentas y responsabilidad en caso de errores y daños. Disponer de información comprensible sobre cómo se han desarrollado los sistemas de IA de alto riesgo y cómo funcionan a lo largo de su vida útil en cuanto a las características generales, las capacidades y las limitaciones del sistema, los algoritmos, los datos, la formación, los ensayos y los procesos de validación utilizados, así como la documentación sobre el sistema de gestión de riesgos pertinente resulta esencial en los usos catalogados como de alto riesgo. De la misma manera que un prospecto de medicamentos proporciona información sobre usos correctos e indebidos o efectos secundarios, abstrayendo al usuario de las descripciones químicas detalladas, un sistema de machine learning debe ofrecer a sus usuarios información significativa que los haga conscientes de la lógica aplicada, así como la importancia y las consecuencias esperadas del procesamiento y los posibles impactos en su vida diaria.

Así, además lo han considerado distintos tribunales sin necesidad de un reglamento de inteligencia artificial.

En 2020, el Tribunal de La Haya[19] ordenó la paralización inmediata de SyRI, al concluir que la legislación por la que se establecía el algoritmo proporcionaba una protección insuficiente contra la intromisión en la vida privada, debido a las medidas desproporcionadas adoptadas para prevenir y castigar el fraude. El tribunal, en ausencia de normas europeas o nacionales que obliguen a desvelar el código fuente que permitieran un mejor control sobre el mismo, o que restrinjan estos usos de la informática en caso de que pueda sospecharse la existencia de estos riesgos, directamente acude al Convenio Europeo de Derechos Humanos (CEDH) y a la protección que el mismo hace sobre la intimidad de las personas para fundamentar la prohibición del uso de la herramienta (COTINO HUESO, 2020[20]).

---

[19] Nota de prensa de la sentencia por el Poder Judicial Holandés. Consultado el 25 de junio de 2023. Disponible en: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-wetgeving-in-strijd-met-het-Europees-Verdrag-voor-de-Rechten-voor-de-Mens.aspx
Sentencia Autoridad Tribunal de Distrito de La Haya (2020). ECLI:ES:RBDHA:2020:865; Número de caso C-09-550982-HA SA 18-388; En inglés: ECLI:NL:RBDHA:2020:1878. Consultado el 25 de junio de 2023. Disponible en: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865

[20] COTINO HUESO, L. (2020). "SyRI, ¿a quién sanciono?": Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020. La Ley privacidad, (4), 2020.

En el caso ***New Jersey v. Francisco Arteaga***[21] se solicita el descubrimiento de la tecnología de reconocimiento facial (FRT) para la identificación del sospechoso en un robo con arma de fuego en una tienda a partir de que supuestamente el gerente de la tienda lo habría reconocido de una visita anterior. Al descubrir que la tecnología FRT tuvo un papel importante en identificación del sospechoso por los testigos, la defensa solicitó su descubrimiento con el código fuente, sus tasas de error, rendimiento, sistema de puntuaciones, lista de parámetros, y otros extremos. Y eso sí, con una declaración de un experto, sus posibles problemas de fiabilidad y la razón de la necesidad del descubrimiento para evaluar sus resultados y rendimiento. De esta manera, se considera que la prueba solicitada está directamente vinculada con la defensa en la posibilidad de sembrar la duda razonable.

Esta sentencia sigue la doctrina fijada por el mismo tribunal en ***State v. Pickett***[22]**.** Se trata de nuevo de una impugnación de un software novedoso HD de genotipificación probabilística para pruebas de ADN. Así, el Tribunal de New Jersey considera que cuando están en juegos las libertades civiles, la revisión independiente del código fuente es fundamental para determinar la fiabilidad. Y en caso de una tecnología novedosa el demandado tiene derecho a acceder a la misma a través de una petición de descubrimiento con orden de protección, siempre que 1) exista una base racional para la petición apoyada por un experto, 2) se solicite una información específica, 3) se pueda salvaguardar la propiedad intelectual mediante orden de protección y 4) cualquier otro factor relevante.

D. Calidad, no discriminación y exactitud de los datos.

En cuanto al grado de calidad de los datos de entrenamiento no se mide simplemente por la acumulación de datos, sino por los parámetros de relevancia, actualidad, fiabilidad, y robustez. En ocasiones, a más datos erróneos, más multiplicación de sesgos, que podrían ser inherentes, si ya existen en los datos que alimentan el sistema, como mala calidad de los datos, datos ausentes, o muestreo selectivo. También podrían ser de representación y medida, debidos a cómo se da formato al conjunto de datos para alimentar al sistema. El conjunto de datos a utilizar ha de analizarse cuidadosamente para evitar dichos riesgos y legitimar su uso si, por ejemplo, el tratamiento se está basando en el interés legítimo.

Los sesgos y discriminaciones en un sistema de IA pueden discriminar injustamente a determinadas personas o grupos, restringiendo potencialmente la disponibilidad de determinados servicios o contenidos, e interfiriendo así en los derechos de las personas, como la libertad de expresión e información, o dando lugar a la exclusión de personas de determinados aspectos de la vida personal, social y profesional.

La sentencia del caso Deliveroo Bolonia[23] aborda la discriminación en las condiciones de acceso al trabajo por parte de los riders a través del algoritmo en una plataforma. Esta sentencia, viene a superar a la de Uber[24] de la Corte Suprema del Reino Unido, porque no sólo analiza la existencia de una relación laboral

---

[21]Superior Court of New Jersey, Appellate Division. (2023). Docket No. A-3078-21 State of New Jersey, V. Francisco Arteaga. Discutida el 15 de mayo de 2023, decidida el 7 de junio de 2023: https://forensicresources.org/resources/new-jersey-v-arteaga-6-7-2023/

[22] State V. Pickett. (2021). Superior Court of New Jersey Appellate Division, 466 N.J. Super. 270 (App. Div. 2021). Disponible en: https://casetext.com/case/state-v-pickett-101

[23] CASTILLO PARRILLA, José Antonio. (2021, 11 de marzo). La discriminación a través del algoritmo en una plataforma. El caso Deliveroo Bolonia y sus implicaciones para el sector público. Consultado el 1 de julio de 2023. Disponible en: https://www.uv.es/catedra-pagoda/es/actualidad/la-discriminacion-traves-del-algoritmo-jose-antonio-castillo-parrilla-1286053802801/Novetat.html?id=1286182093538 Puede consultarse la sentencia aquí, TRIBUNALE ORDINARIO di BOLOGNA Sezione Lavoro Causa n. r.g. 2949/2019 27 de noviembre de 2020 FILCAMS CGIL BOLOGNA. NIDIL CGIL BOLOGNA, FILT CGIL BOLOGNA Contro DELIVEROO ITALIA S.R.L https://www.algoritmolegal.com/wp-content/uploads/2021/01/Sentencia-Bologna-Italia-Deliveroo-dic-2020-Original-italiano.pdf

[24] Uber BV and others (Appellants) v Aslam and others (Respondents). (2021, 19 de febrero). Heard on 21 and 22 July 2020. Consultado el 1 de julio de 2023. Disponible en: https://www.supremecourt.uk/cases/uksc-2019-0029.html

de los riders sino que además entra en el análisis de la posible discriminación del algoritmo respecto a las condiciones de acceso a las sesiones de trabajo por los repartidores y en particular de los parámetros de tratamiento del llamado "ranking reputacional". Así, se les asigna un horario de trabajo, dependiendo de un scoring en fiabilidad y disponibilidad. El índice de fiabilidad sería el número de veces en que el trabajador no habría cumplido con su sesión previamente reservada y la disponibilidad tiene en cuenta el número de veces que está disponible en los horarios de mayor demanda (noches de los fines de semana). Así, el algoritmo no permitiría las ausencias al trabajo por motivos de huelga, enfermedad, o por ejemplo cuidado de familiares o hijos, de tal manera que estaría impidiendo en la práctica el ejercicio de derechos, permisos y licencias reconocidos legalmente. El código se convierte en la ley como dice LESSIG[25]. Señala el tribunal de Bolonia, que Deliveroo no sabe y no quiere saber los motivos por los que el corredor cancela su reserva o no participa en una sesión reservada y no cancelada. Pero es precisamente en esta "inconsciencia" (como lo define Deliveroo) y "ceguera" (como lo definen los solicitantes) del programa de procesamiento de estadísticas de cada corredor que alberga el potencial discriminatorio del mismo.

Otro de los principios fundamentales de la protección de datos es la "exactitud" de los mismos, que se define en el artículo 5.1.d del RGPD. En el caso de tratamientos que incorporan soluciones IA, la existencia de sesgos en los modelos de inferencia está íntimamente ligado con la exactitud o calidad del dato. Una de las principales acusaciones por ejemplo a ChatGPT es la creación de información falsa, errónea o inexacta, lo que iría contra ese principio de privacidad. El propio sistema reconoce al hacer log in una serie de limitaciones:

3. Puede generar ocasionalmente información incorrecta

4. Puede generar ocasionalmente instrucciones perjudiciales o contenidos tendenciosos

5. Conocimiento limitado del mundo y los acontecimientos posteriores a 2021

Un locutor de radio en Georgia, Mark Walters, ha demandado a la compañía después de que el sistema le acusara de defraudar y malversar fondos[26]. Y este tipo de acciones judiciales se suceden[27].

En un sistema de IA generativa o modelos fundacionales, deberían incluirse salvaguardias adecuadas que eviten la inexactitud de los datos de entrada y protejan del impacto de datos inexactos, con estrategias "desde el diseño" en la ejecución del tratamiento, y su efectividad debe revisarse y actualizarse cuando sea necesario. Cuando la IA evoluciona de ser un elemento experimental a un producto, es necesario incorporar las mismas garantías que se le reclaman a cualquier otro servicio tecnológico. Al igual que los medicamentos para acceder al mercado deben superar una evaluación favorable de su calidad, seguridad y eficacia, este tipo de sistemas debería ser igual con una previa evaluación de impacto, que se establece de manera preceptiva en el artículo 35.3.a RGPD, cuando se realice elaboración de perfiles basados en tratamientos automatizados. Sin embargo, la sensación es que todavía en ciertas empresas sigue imperando el clásico lema de Silicon Valley *"move fast and break things"* y que las pruebas y testeos se realizan en el propio mercado, siendo los propios usuarios los *betatesters.* Así, no se trataría sólo de que si algo es gratis, el producto eres tú, y hemos estado entrenando con nuestros datos los grandes modelos de IA, sino que además, la función de evaluación, testeo y detección de fallos la están realizando los propios usuarios en el mercado sin una previa evaluación por parte de la compañía. De esta manera, no sólo no serían tecnologías maduras, y con las que por consiguiente, hay que guardar las necesarias reservas, sino que podrían no cumplir con los requisitos básicos de "accountability", transparencia y legalidad

[25] LESSIG, Lawrence. (2009). El código 2.0. Madrid. Proyecto editorial Traficantes de Sueños.
[26] VINCENT, James. (2023). OpenAI sued for defamation after ChatGPT fabricates legal accusations against radio host. The Verge. 9 de junio de 2023. Consultado el 1 de agosto de 2023. Disponible en: https://www.theverge.com/2023/6/9/23755057/openai-chatgpt-false-information-defamation-lawsuit
[27] HSU, Portiffany. (2023, 3 de agosto). What Can You Do When A.I. Lies About You? The New York Times. Consultado el 4 de agosto de 2023. Disponible en: https://www.nytimes.com/2023/08/03/business/media/ai-defamation-lies-accuracy.html

El Garante italiano le requirió una herramienta a través de la cual solicitar y obtener la corrección de cualquier dato personal que les concierne procesado de manera inexacta en la generación de contenido o, si esto resulta imposible en el estado de la técnica, la cancelación de sus datos personales. A raíz de la intervención de la autoridad de control, OpenAI modificó su política de privacidad[28] según la cual:

Si observa que la salida de ChatGPT contiene información objetivamente inexacta sobre usted y desea que corrijamos la inexactitud, puede enviar una solicitud de corrección a dsar@openai.com. Dada la complejidad técnica de cómo funcionan nuestros modelos, es posible que no podamos corregir la inexactitud en todos los casos. En ese caso, puede solicitar que eliminemos su información personal de la salida de ChatGPT completando este formulario .

De la misma manera se le requirió para garantizar y respetar los derechos a la información, el derecho de acceso, el derecho a oponerse al tratamiento y el derecho a la supresión de datos personales.

E. Supervisión humana.

Otro de los principios fundamentales en la IA es el principio de autonomía o preservación de la supervisión humana: el ser humano no puede estar subordinado o coartado por la IA debiendo mantener de manera efectiva y completa su autodeterminación.

En este sentido, la Carta de Derechos Digitales en su Título XVIII 6 d) establece *"El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente".* Y XXV, *3. Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial.*

Debe garantizarse el derecho a no ser objeto de una decisión únicamente automatizada, a ser informado de la decisión automatizada, el derecho a impugnar o revisar las decisiones automatizadas o algorítmicas y a solicitar una supervisión e intervención humana (Art. 22 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 adoptadas el 3 de octubre de 2017, revisadas por última vez y adoptadas el 6 de febrero de 2018 del antiguo Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE.Capítulo XXV, Carta Derechos Digitales). Y en particular, el artículo 22.4 establece que las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar, no se basarán en las categorías especiales de datos personales (ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico) salvo que medie el consentimiento del interesado o el tratamiento sea necesario por razones de un interés público esencial.

Este derecho a no estar sujeto a la toma de decisiones automatizada finalmente se está considerando por primera vez ante el Tribunal de Justicia de la Unión Europea en el Asunto C-634/21 OQ contra Land Hessen, con intervención de: SCHUFA Holding AG [Petición de decisión prejudicial planteada por el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania). Así, en un supuesto donde se realizó a un ciudadano un *scoring* que sirvió de base para denegar un crédito, el Abogado General en sus conclusiones ha informado que el interesado no sólo tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernan, sino también otra información, como la existencia de decisiones automatizadas, incluida la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado, considerando ésta en el sentido de que incluya explicaciones suficientemente detalladas sobre el método utilizado para el cálculo del score y

[28] Política de privacidad Chatgpt OpenAI. Consultado 1 de agosto de 2023. Disponible en:

sobre las razones y factores que han conducido a un resultado determinado en la toma de decisiones y su importancia desde el punto de vista agregado a fin de poder impugnar la decisión. Esto último es, las explicaciones suficientemente detalladas sobre el método utilizado para el cálculo del score y sobre las razones que han conducido a un resultado determinado.

La protección del secreto comercial o de la propiedad intelectual constituye, en principio, un motivo legítimo pero no puede justificar la denegación total de información.

Y es que en general, el perfilado implica una serie de deducciones estadísticas para inferir algo sobre un individuo o realizar un tipo de evaluación o juicio sobre la base de un análisis de las cualidades de otros que parecen similares estadísticamente y puede tener efectos en las personas interesadas al incluirlas en categorías predeterminadas, a menudo sin su conocimiento; privándolos de manera injustificada del acceso a ciertos bienes o servicios, violando como consecuencia el principio de no discriminación.

Como dijo el Comité de Ministros del Consejo de Europa[29] *"cada vez más, los medios computacionales hacen posible inferir información íntima y detallada sobre individuos a partir de datos fácilmente disponibles. Esto apoya la clasificación de los individuos en categorías, lo que refuerza las diferentes formas de discriminación y segregación social, cultural, religiosa, legal y económica. También facilita la microfocalización de personas en función de los perfiles de maneras que pueden afectar profundamente sus vidas".*

En resumen, la IA debe ser antropocéntrica con propósitos éticos de beneficiencia, no maleficencia, supervisión humana, justicia y explicabilidad para ser un sistema confiable. Además, debe respetar los derechos fundamentales y prestar particular atención a grupos vulnerables para no caer en sesgos o discriminaciones, debiendo estar particularmente vigilantes en aquellas áreas críticas o de alto riesgo.

3. ASPECTOS ORGANIZATIVOS, DE AUDITORÍA Y DE SUPERVISIÓN.

En cuanto a las organizaciones, al igual que el Delegado de Protección de Datos (DPD), no siendo siempre obligatorio, es un elemento clave para garantizar el cumplimiento y la gestión del riesgo para los derechos y libertades de los interesados, en el caso de la IA, debido al gran número de obligaciones de documentación, gestión y análisis de riesgos, evaluación de conformidad, archivos y registros y verificación del diseño, desarrollo y vigilancia posterior, parece lógico que se desarrolle una figura similar al DPD, que ya se está llamando AICO-*Artificial Intelligence Compliance Officer*, AIO *Artificial Intelligence Officer* o RAI *Responsible AI Officer.* Así, los más próximos a poder asumir estas funciones pueden ser los DPDs, CISOs o perfiles de Data Scientist especializados en cuestiones éticas que se formen a nivel de cumplimiento normativo (al igual que un DPD no tiene que ser necesariamente jurista).

Por último, se hace necesaria la creación de las autoridades de supervisión a nivel europeo y español, el diseño de sus estatutos, la coordinación con otras autoridades como la AEPD y el supervisor europeo. No queda claro cómo se van a articular una Oficina Europea de IA (EAI Office), los supervisores nacionales de IA (AESIA), los Coordinadores de Servicios Digitales de la *Digital Markets Act*, la Junta Europea de Servicios Digitales (las grandes plataformas se someterán a la DSA con entrada en vigor desde 17 de febrero de 2024 y al AI Act como sistemas de alto riesgo), el European Data Protection Supervisor y la AEPD.

La Oficina Europea de IA debe actuar con plena independencia y encargarse de diversas tareas de asesoramiento y coordinación, en particular la emisión de dictámenes, recomendaciones, informes de asesoramiento u orientaciones sobre asuntos relacionados con la aplicación de este Reglamento. Cada Estado miembro debe designar a una autoridad nacional de supervisión que se encargue de supervisar la

[29] Declaración del Comité de Ministros sobre las capacidades de manipulación de los procesos algorítmicos. (2019, 13 de febrero). Adoptada en la 1337 reunión. Consultado el 28 de enero de 2023. Disponible en: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

aplicación y ejecución del presente Reglamento y de representar a su Estado miembro en el consejo de administración de la Oficina de IA, con el fin de incrementar la eficiencia en términos de los Estados miembros y establecer un punto de contacto oficial con el público y otros homólogos en los Estados miembros y la Unión. Y sobre todo, cada autoridad nacional de supervisión debe actuar con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el próximo reglamento europeo, garantizando total transparencia y rindiendo cuentas ante las autoridades europeas. De tal manera que, por ejemplo, su director ejecutivo no pedirá ni recibirá instrucciones de ningún Gobierno o cualquier otro organismo y por lo tanto debe ser plenamente independiente.

Respecto a la autoridad española, la AESIA, su adjudicación está pendiente de sentencia por haber sido recurrida ante la Sala Tercera del Tribunal Supremo. Siendo la primera agencia mundial de supervisión de IA y una institución a la cual reglamentariamente se le exige un alto nivel de transparencia, no se ha sometido a debate público (a diferencia de la normativa del Sandbox[30]) habiéndose publicado sus estatutos mediante Real Decreto el sábado 2 de septiembre[31]. La AESIA, a diferencia de otras autoridades de control no exige para el nombramiento de su director y adjunto, unos requisitos profesionales mayores que "la titulación, la experiencia y las aptitudes, en particular en el ámbito de la inteligencia artificial". Para por ejemplo ser Director de la Agencia Española de Protección de Datos se requiere "reconocida competencia profesional" y "candidatas que su independencia, conducta intachable e integridad deben estar fuera de toda duda". Para ser Presidente del CGPJ, se requiera haber sido magistrado del Tribunal Supremo o jurista de reconocida competencia con más de veinticinco años de antigüedad en el ejercicio de su profesión[32]. Mientras que el presidente de la CNMC[33] será elegido entre personas de reconocido prestigio y competencia profesional, en la Agencia Española de Seguridad Aérea[34] se tendrán en cuenta criterios de competencia profesional y experiencia y en el Consejo de Seguridad Nuclear, "conocida solvencia"[35].

En el caso de la AEPD, la Presidencia y su Adjunto deben someterse a comparecencia y votación pública en la Comisión de Justicia del Congreso de los Diputados[36]. Igual ocurre con los miembros del Consejo, el Presidente y el Vicepresidente, de la CNMC (Art. 15) o del Consejo de Seguridad Nuclear (Art. 25).

Nada se establece de duración del mandato en la AESIA de su Dirección ni de las causas objetivas de separación del cargo, a diferencia por ejemplo de los 5 años en la AEPD (Art. 48), 6 años en la CNMC (Art. 15) o en el Banco de España[37].

El Consejo Rector de la AESIA está compuesto por el Director, 6 subdirectores generales de ministerios y un experto. Lo cierto es que el Foro Consultivo a nivel Europeo tendrá una composición equilibrada de partes interesadas, incluidos la industria, las empresas emergentes, las pymes, la sociedad civil, los interlocutores sociales y el mundo académico. En nuestro país el Consejo Rector de la Agencia Estatal de

---

[30] Audiencia pública sobre el Real Decreto que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial. Consultado 1 julio de 2023. Disponible en: https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/audiencia_entorno_controlado_pruebas_ensayo_cumplimiento_normas_armonizadas_IA.aspx

[31] Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial. BOE 2 Septiembre 2023. LA LEY 24251/2023

[32] Art. 586 Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. BOE 2 Julio 1985. LA LEY 1694/1985

[33] Art. 15 Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. BOE 5 Junio 2013. LA LEY 8683/2013

[34] Art. 25 Real Decreto 184/2008, de 8 de febrero, por el que se aprueba el Estatuto de la Agencia Estatal de Seguridad Aérea. BOE 14 Febrero 2008. LA LEY 1060/2008

[35] Art. 25 Real Decreto 1440/2010, de 5 de noviembre, por el que se aprueba el Estatuto del Consejo de Seguridad Nuclear. BOE 22 Noviembre 2010. LA LEY 23147/2010

[36] Art.48 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE 6 Diciembre 2018. LA LEY 19303/2018

[37] Art. 38 Resolución de 28 de marzo de 2000, del Consejo de Gobierno del Banco de España, por la que se aprueba el Reglamento Interno del Banco de España. BOE 6 Abril 2000. LA LEY 1514/2000

Seguridad Aérea (AESA) y los miembros del Consejo de la CNMC tienen una composición equilibrada.

Como decíamos, a nivel de coordinación de igual manera, existirán el European Data Protection Board, el Foro Consultivo de IA (AI Advisory Forum) o el Centro Europeo de Transparencia Algorítmica (ECAT) y los sandbox, cuyas recomendaciones, buenas prácticas, pautas u opiniones también deberán (se entiende) coordinarse entre sí.

También deberán ponerse en marcha los registros de archivos y de operadores de alto riesgo, adopción de sistemas estandarizados de auditoría de algoritmos y cumplimiento normativo y la implementación del sandbox o banco de pruebas para comenzar a ponerlos en práctica, formación para auditores que sean capaces de evaluar la implementación y que previamente hayan sido acreditados como organismos de evaluación. O por ejemplo, ¿cómo se coordinará un sello español de la IA con un sello europeo y unas normas estandarizadas internacionales y qué valor añadido aportará nuestro marcado en un mundo globalizado? ¿cómo se va a coordinar por ejemplo el el Europrivacy o sello europeo de protección con el marcado europeo de inteligencia artificial, puesto que el segundo no tiene por qué suponer el cumplimiento del primero?, ¿y las normas estandarizadas?

En cuanto a los actos**,** nada se establece en el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial sobre su régimen de actos administrativos: circulares, dictámenes, informes, potestad de inspección, requerimientos de información, procedimiento sancionador, sanciones, denuncias, reclamaciones, sujetos responsables, infracciones, régimen normativo interno, código de conducta, coordinación con oficina europea IA, posibles conflictos de competencia AESIA- AEPD, e incluso el procedimiento y competencia para la impugnación de los actos o sanciones de la AESIA, que no dejan de ser actos administrativos y deberán ser objeto de posible impugnación judicial.

Por todo ello, podemos concluir, que al igual que el borrador de Real Decreto de Sandbox está limitado en el tiempo hasta que se adopte el Reglamento de la Unión Europea (Art. 28), la normativa interna de la primera agencia de supervisión de inteligencia artificial mundial será susceptible de reforma y mejora próximamente para su adaptación una vez se produzca la aprobación del Reglamento Europeo y su constitución como entidad supervisora y sancionadora independiente ya que de lo contrario se podría incurrir en un incumplimiento de la norma europea, apreciable tanto por la Comisión[38] como por el TJUE en virtud de cuestión prejudicial por cualquier recurso jurisdiccional frente a una sanción de dicha institución por ejemplo.

4. CONCLUSIONES

El cumplimiento normativo de la IA Act irá de la mano del RGPD y LOPDGDD y para ello deberán tener una base de legitimación y un tratamiento de los datos adecuado, pertinente y proporcional a su finalidad.

Estas tecnologías, independientemente del ámbito en el que se desarrollen, desplieguen y utilicen, deben ser desarrolladas desde el diseño de manera segura, rastreable, técnicamente sólida, fiable, ética y jurídicamente vinculante y ser objeto de un control y una supervisión independientes. Y para ello resultan esenciales las condiciones de explicabilidad, auditabilidad, trazabilidad y transparencia. Además en el caso de decisiones automatizadas deberá existir la posibilidad de impugnación y supervisión humana.

Y es esencial garantizar este tipo de principios de la privacidad desde el diseño y por defecto en todo el ciclo de vida de la IA como parte de un enfoque global de "ética desde el diseño".

La IA debe ser antropocéntrica con propósitos éticos de beneficiencia, no maleficencia, supervisión

[38] Alarcón, N. (2023, 18 de octubre). Bruselas lleva España a la Justicia europea por la falta de independencia de Adif. El Confidencial. Consultado el 23 de octubre de 2023. Disponible en: Bruselas lleva España a la Justicia europea por la falta de independencia de Adif (elconfidencial.com)

humana, justicia y explicabilidad para ser un sistema confiable. Además, debe respetar los derechos fundamentales y prestar particular atención a grupos vulnerables para no caer en sesgos o discriminaciones, debiendo estar particularmente vigilantes en aquellas áreas críticas o de alto riesgo.

Además, como podemos ver, cuando uno se asoma a la IA, aparecen conceptos bien conocidos en privacidad: análisis de riesgos, evaluación de impacto, normas de estandarización, sello europeo, autoridad de supervisión, órganos consultivos, delegado de protección, etc.

Respecto a la futura entidad de supervisión, la AESIA, podemos concluir, que al igual que el borrador de Real Decreto de Sandbox está limitado en el tiempo hasta que se adopte el Reglamento de la Unión Europea (Art. 28), la normativa interna de la primera agencia de supervisión de inteligencia artificial mundial será susceptible de reforma y mejora próximamente para su adaptación una vez se produzca la aprobación del Reglamento Europeo.

Una estrecha conexión de ambos ámbitos condenados a entenderse. El Secretario General del SEPD, Leonardo Cervera-Navas, destacó en una conferencia el 7 de julio de 2023 que *"el Reglamento sobre Inteligencia Artificial y el Reglamento General de Protección de Datos deben ir de la mano en beneficio de todos. Tenemos que adoptar la tecnología de acuerdo con los valores de la UE".*

BIBLIOGRAFÍA:

- CASTILLO PARRILLA, José Antonio. (2021, 11 de marzo). La discriminación a través del algoritmo en una plataforma. El caso Deliveroo Bolonia y sus implicaciones para el sector público. Consultado el 1 de julio de 2023. Disponible en: https://www.uv.es/catedra-pagoda/es/actualidad/la-discriminacion-traves-del-algoritmo-jose-antonio-castillo-parrilla-1286053802801/Novetat.html?id=1286182093538

- COTINO HUESO, L. (2020). "SyRI, ¿a quién sanciono?": Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020. La Ley privacidad, (4), 2020.

- ESTEBAN RUIZ, Adaya María. (2022, 21 de noviembre). Entrenamiento de redes neuronales con datos de fuentes públicas, web scrapping y el problema de la falta de transparencia y trazabilidad de la información (1). Diario La Ley.

- MARTÍNEZ MARTÍNEZ, R. (2019). Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo. Revista catalana de dret públic, 58, 64-81. Consultado el 1 de julio de 2023. Disponible en: http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-rcdp.i58.2019.3317