Telefónica Tech

Implicaciones en privacidad y seguridad de la convergencia entre IoT, Big Data e IA

telefonicatech.com

Centro de innovación en ciberseguridad de IoT y Smart Cities de Telefónica Tech Cyber Security & Cloud

Implicaciones en privacidad y seguridad de la convergencia entre IoT, Big Data e IA.

València, 2021

La presente obra colectiva ha sido concebida en el marco del Centro de innovación en ciberseguridad de IoT y Smart Cities de Telefónica Tech Ciber Security & Cloud en València.

La misma ha sido redactada por el equipo de Govertis Advisory Services, empresa de Telefónica Tech.

Coordinadores:

Eduard Chaveli Donet, *Head of Consulting Strategy*

María Loza Corera, *Lead Legal Advisor (New Challenges)*

Joan Figueras Tugas, *Lead Security & GRC Advisor*

Autores:

Pablo Ballarin Usieto, *Senior Advisor (Security & GRC)*

Ángel Escudero Molina, *Senior Advisor (Security & GRC)*

Joan Figueras Tugas, *Lead Advisor (Security & GRC)*

María Loza Corera, *Lead Legal Advisor (New Challenges)*

Jordi Morera Torres, *Lead Legal Advisor (Compliance)*

Andreu Yakubuv-Trembach, *Junior Advisor (Data Protection)*

De la revisión de la obra han participado **Vicente Segura Gualde**, *Head of IoT Security at Telefónica*, y **David Prieto Marqués,** *Head of Identity at Telefónica y Responsable del Centro de Telefónica Tech en Valencia.*

Índice

Presentación

La presencia de los productos y servicios relacionados con el paradigma del IoT es ya una realidad. Se espera que haya más de 30 miles de billones[1] de dispositivos IoT conectados en 2023, lo que supone, aproximadamente, tres dispositivos por habitante. Emergen nuevas aplicaciones del IoT para prácticamente todo tipo de industria. Las características de la conectividad 5G impactan en la aceleración del desarrollo de nuevas capacidades funcionales sobre aplicaciones ya conocidas del IoT como pueden ser: coche conectado, realidad virtual y aumentada, *wereables* aplicados al *fitness* y e-*health*, o la familia de aplicaciones '*smart*' (Smart-City, Smart-Port, Smart-Village, Smart-Agro…), entre muchas otras.

En estos ejemplos, se materializa la contribución de tres de las tecnologías más relevantes de la última década: IoT, Big Data e Inteligencia Artificial. La mayoría de los casos de uso del IoT no se podrían concebir sin la participación de los otros dos elementos.

El IoT es la principal fuente de información. Los miles de dispositivos conectados generan millones de datos. Estos datos son optimizados y analizados por la tecnología *Big Data*. El *Machine Learning* (ML) y la Inteligencia Artificial (IA) utilizan los *datasets* para aportar valor a los propios servicios IoT o a otras áreas de negocio de las plataformas IoT produciéndose así un círculo virtuoso entre las tres tecnologías.

Todo este ecosistema, con su alto grado de complejidad, requiere de mecanismos de gobierno que permitan mantener el control sobre dispositivos, sistemas, procesos y datos, de forma que podamos garantizar el correcto funcionamiento de cada elemento bajo diversos puntos de vista: ético, legal, técnico, económico…

A modo de un director de orquesta, el Gobierno del Dato considera por igual los aspectos de negocio, organizativos y técnicos; y ayuda a que trabajen de forma conjunta para obtener un todo armonioso.

Los beneficios para la sociedad de la transformación digital tienen su fundamento, en buena medida, en la aplicación de esta tríada tecnológica para aportar soluciones transformadoras en cualquiera de los ámbitos de la sociedad: profesional, negocios, personal, sanitario, ocio etc.

Sin embargo, esta misma potencialidad tiene como contrapunto la proliferación de nuevas amenazas o la maximización de algunas ya existentes, que pueden afectar a las personas. Comenzando por los riesgos que pueden impactar en la privacidad y la seguridad de los individuos cuyos datos son recogidos y procesados por estas tecnologías conforme a criterios de negocio que deben estar alineados con la necesidad de preservar los derechos y libertades de los ciudadanos.

Además del cumplimiento normativo tanto en materia de seguridad como de privacidad, el componente ético debe prevalecer en la toma de decisiones en toda la cadena de valor de las soluciones tecnológicas y en todo su ciclo de vida.

[1] LAROVICI, Y., Top ten IoT use cases, julio 2020, en *IoT Evolution* https://www.iotevolutionworld.com/iot/articles/446032-top-10-iot-use-cases.htm#:~:text=Another%20IoT%20use%20case%20is,are%20increasingly%20global%20and%20complex.&text=Low%2Dpower%20IoT%20devices%20are,to%20track%20shipping%20container%20openings

Esta obra va dirigida a todos aquellos que pueden tener alguna responsabilidad en la concepción, diseño, implementación y explotación de cualquier solución tecnológica basada en alguna de estas tres tecnologías. El lector podrá encontrar una recopilación de los potenciales riesgos relacionados con el IoT, el *Big Data* y la Inteligencia Artificial, catalogados en distintos ámbitos como son el ético, el legal, la ciberseguridad y privacidad. El informe ofrece una visión sobre los desafíos que plantea la normalización y presenta el estado del arte de la regulación que les afecta y cómo el Gobierno del Dato contribuye a la consecución de los objetivos éticos, técnicos y culturales marcados.

Parte 1: La convergencia entre las tres tecnologías

1. Elementos y conceptos básicos.

BIG DATA

En la bibliografía de teoría de la información se entiende por datos los caracteres o símbolos de comunicaciones que pueden formalizarse y reproducirse (a voluntad) y que son fácilmente transportables con ayuda de medios técnicos adecuados para ello. Los datos como tales no tienen ningún sentido intrínseco, son el "petróleo crudo". Pero pueden ser portadores y/o facilitadores de información, incluida la codificada, adquiriendo especial sentido en un contexto de comunicación (entre personas y/o entre "cosas")[2].

Al Big Data frecuentemente se le caracteriza a través de la célebre definición de las tres 'V'[3]: **Volumen**, **Variedad** y **Velocidad**. Esto es, manejar un gran volumen de información (en relación con la cantidad), procesar los datos a gran velocidad o en tiempo real (rapidez en la obtención de resultados interpretativos) e integrar gran variedad de fuentes de información para, a través de diferentes técnicas analíticas, generar conocimiento y valor. Además, algunos autores y organizaciones han añadido **'v'** adicionales para definir de forma más precisa al Big Data. Por ejemplo, **Veracidad** (la calidad de los datos capturados es clave), **Variabilidad** (el significado de los datos cambia frecuentemente y se pueden producir inconsistencias que se han de manejar) y **Valor** (los ingresos o beneficios del Big Data)[4] lo cual, por otro lado, ha sido criticado por ser características más propias de los datos en sí mismos que del propio concepto de Big Data.

Este concepto de macrodatos, además de referir a la realidad de los datos masivos, apunta a la gran oportunidad que se ofrece desde que existe la capacidad técnica requerida para su análisis y aprovechamiento, permitiendo obtener conclusiones rápidamente sobre la probabilidad de que determinados sucesos o patrones puedan ocurrir. Es aquí donde el Big Data puede permitirnos una explotación más eficiente de nuestro negocio si adoptamos desde un inicio una estrategia con objetivos de negocio concretos. Sin embargo, implementar estas y otras soluciones tecnológicas innovadoras en pro de los intereses del negocio ha de respetar los límites legales y éticos, algo que abordaremos en apartados posteriores.

INTERNET DE LAS COSAS (IoT)

Internet de las Cosas o de los objetos, también conocido por sus siglas en inglés como *IoT* (*Internet of Things*), ha sido definida como aquella "infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos («objetos» como tales, u objetos vinculados a otros objetos o individuos)

---

[2] HOFFMANN-RIEM, W., *Big Data. Desafíos también para el Derecho*, Pamplona: Civitas, 2018, pág. 51.

[3] LANEY, D., "3D Data Management: Controlling Data Volume, Velocity, and Variety", *Application Delivery Strategies*, META Group Inc, fichero 949, 6 de febrero de 2001, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

[4] AEPD, *Código de buenas prácticas en protección de datos para proyectos Big Data*, Coords.: Emilio Aced, M. Rosario Heras y Carlos Alberto Sáiz, 2019, pág 3, https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

registran, someten a tratamiento, almacenan y transfieren datos que al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red"[5].

El desarrollo de las últimas dos décadas de Internet de las Cosas ha sido esencial para configurar el circundante ambiente del progreso tecnológico. La actualidad de una Internet global supone que desde 2016, el número de objetos conectados supera con creces al número de habitantes. Los miles de millones de objetos cotidianos interconectados en la red tienen tres fuentes principales de datos: los que facilita voluntariamente el usuario, los que perciben del entorno (ubicación, velocidad, temperatura, tensión arterial, imagen, sonido, etc.) y los que genera el dispositivo con su funcionamiento.

La estructura de IoT supera la barrera entre los objetos en el mundo físico y con ello, se consigue pasar de la existencia de objetos tradicionales (considerados pasivos) a objetos inteligentes (activos), recopilando información y transformándola en datos que más tarde, serán procesados y enviados a Internet[6]. IoT cumple con el objetivo de optimizar los recursos, es decir, de hacernos capaces de monitorizar, contar y localizar todo lo relativo a nuestras "cosas", nuestros factores productivos y nosotros mismos, reduciendo en gran medida gastos, pérdidas y costes, así como conociendo al detalle sobre el estado de todo aquello.

De hecho, cobra mayor sentido pasar a utilizar la nueva denominación '**Internet del Todo'**, que engloba lo que entendemos por Internet de las Cosas y su variante sectorial de "Internet de las cosas robóticas" (***IoRT***, del inglés "*Internet of Robotic Things*"), ampliando las miras hacia la realidad de conexión en red de cosas, seres vivos, sus procesos y datos, todo con una mayor capacidad técnica, aplicación "smart" y automatización, al tiempo que asumiendo una nueva dimensión en la comunicación de humanos a humanos (H2H)[7].

INTELIGENCIA ARTIFICIAL (IA)

La tendencia humana a crear réplicas propias para las tareas que requieren un ejercicio de inteligencia es bastante antigua y son muchos los aspectos históricos sobre la conceptualización de Inteligencia Artificial (*Artificial Intelligence*), en adelante, IA. No obstante, lo anterior, no existe un concepto unánime o generalmente aceptado de IA. De hecho, no hay una concepción unívoca sobre la IA.

En la Comisión Europea entienden que "el término inteligencia artificial se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos"[8].

---

[5] GT29, *Dictamen 8/2014 sobre la evolución reciente del Internet de los Objetos*, elaborado por el Grupo de Trabajo sobre protección de datos del artículo 29 (Unión Europea), 16 septiembre de 2014, pág. 4. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf

[6] BARRIO, M., Internet de las Cosas. Madrid: Reus, 2018, pág. 21.

[7] KALYANI, V.L., SHRAMA., D., "IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication", JMEIT, v. 2, nº. 6, diciembre de 2015, http://www.jmeit.com/JMEIT%20Vol%202%20Issue%206%20Dec%202015/JMEITDEC0206003.pdf

[8] COMISIÓN EUROPEA, "Inteligencia artificial para Europa", Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, COM(2018) 237 final, 25 de abril de 2018. https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF

Posteriormente, el Grupo Independiente de Expertos de Alto Nivel en Inteligencia Artificial (AI-HLEG, por sus siglas en inglés) de la Comisión Europea, ha profundizado conceptualizando los sistemas de inteligencia artificial (IA) como sistemas de software (y posiblemente también de hardware) diseñados por los humanos que, dado un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno a través de la adquisición de los datos, interpretación de los datos estructurados o no estructurados recogidos, razonamiento sobre el conocimiento, o procesamiento la información derivada de estos datos, y decidir la/s mejor/es medida/s a adoptar para alcanzar el objetivo fijado. Tal y como indican, "los sistemas de IA pueden utilizar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento analizando cómo el entorno se ve afectado por sus acciones anteriores"[9].

Por otra parte, el *Joint Research Centre* de la Comisión Europea señala cuatro características que se comprueban al hablar de Inteligencia Artificial[10]:

- percepción del entorno y la complejidad del mundo real;
- tratamiento de la información (recolección e interpretación de los inputs);
- toma de decisiones que incluye aspectos como el razonamiento, el aprendizaje y llevar a cabo acciones;
- y consecución de objetivos predefinidos.

En la Propuesta de Reglamento europeo sobre Inteligencia Artificial[11] la definición dada para definir un sistema de IA contempla dichas características: "software that is developed with one or more of the techniques and approaches (...) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

A su vez, existen diferentes tipos o categorías de IA en función de su alcance y ámbito de aplicación. Podemos hablar de dos tipos de IA[12]: la denominada '**IA débil'** o **'estrecha' (*weak*)**, que sería aquella que se concreta o especializa en una determinada tarea (por ejemplo, un asistente virtual como Siri o Cortana); y la '**IA fuerte' (*strong*),** que sería capaz de acercarse al objetivo de la IA, realizando actividades como si de un humano se tratase. Se diferencia de la anterior, por tanto, en que tiene iniciativa propia. También se habla de una '**super inteligencia artificial'**, en el sentido de aquella que llegará a ser igual o mayor que la inteligencia humana.

[9] COMISIÓN EUROPEA, A *Definition of AI: Main capabilities and disciplines*, por el grupo de expertos de alto nivel en Inteligencia Artificial, 2018, pág. 6. https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[10] SAMOILI, S., LÓPEZ COBO, M., GÓMEZ, E., DE PRATO, G., MARTÍNEZ-PLUMED, F., & DELIPETREV, B., AI Watch. *Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*, Luxembourg: Publications Office of the European Union, 2020, pág. 8. https://ec.europa.eu/jrc/en/publication/ai-watch-defining-artificial-intelligence

N.B.: *En dicho informe técnico, se parte de un análisis de 29 políticas e informes institucionales (por ejemplo, intentos de estandarización o estrategias nacionales), 23 publicaciones de investigación y 3 informes de mercado, desde 1955 hasta la fecha de publicación del informe.*

[11] Artículo 3 (1), 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. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=ES

[12] LOZA CORERA, M., "Big data e inteligencia artificial", Govertis Advisory Services, 4 de diciembre 2018, https://www.govertis.com/big-data-e-inteligencia-artificial

Por su parte, la AEPD también distingue tres tipos de inteligencia artificial, pero con otras denominaciones[13]: la IA fuerte, general y débil, siendo la general la que podría resolver cualquier tarea intelectual resoluble por un ser humano y por tanto, equivaldría a la anteriormente conceptuada como fuerte; al tiempo que la fuerte equivaldría a la anteriormente mencionada como superinteligencia, aquella que iría más allá de las capacidades humanas.

Categorías de IA	***Categorías de IA según la AEPD***
Débil (estrecha)	Débil
Fuerte	General
Superinteligencia	Fuerte

Figura 1: Tabla correspondencia entre las categorías de IA según distintas fuentes bibliográficas. Elaboración propia.

Es en este punto donde cobran vital importancia los **algoritmos**, como llamamos al conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas[14]. Para lo que nos ocupa, los algoritmos son partes de sistemas digitales complejos de toma de decisiones, compuestos por software y hardware, e integrados en sistemas de información sociotecnológicos.

Existen diferentes técnicas en función de los avances obtenidos[15]. Así, el *Machine Learning (ML)* o **aprendizaje automático**, también llamado de máquinas, supone dotar a la computadora de la capacidad de mejorar o aprender por sí misma, sin tener que haber sido programada explícitamente para ello[16]. Tal y como afirma la AEPD "el aprendizaje automático está relacionado con las técnicas de minería de datos, optimización y big data" [17].

Por su parte, el *Deep Learning* (DL) o **aprendizaje profundo**, constituye una rama del ML, pues ambas son técnicas de aprendizaje automático, pero con la diferencia de que el DL se basa en redes neuronales o

[13] AEPD, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020, p. 5. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[14] SÁNCHEZ CHINCHÓN, A., "Los algoritmos nos facilitan la vida: así funcionan", Telefónica Think Big Empresas, 21 de noviembre de 2016, https://empresas.blogthinkbig.com/los-algoritmos-nos-facilitan-la-vida-asi-funcionan

[15] LOZA CORERA, M., Op. Cit.

[16] RECUERO DE LOS SANTOS, P., "Tipos de aprendizaje en Machine Learning: supervisado y no supervisado", Telefónica Think Big Empresas, 16 de noviembre de 2017, https://empresas.blogthinkbig.com/que-algoritmo-elegir-en-ml-aprendizaje

[17] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial..., Op.Cit.

procesamiento de datos por capas, tratando de emular el funcionamiento del cerebro humano. En los últimos años el DL ha supuesto una enorme revolución gracias a un mayor abaratamiento y accesibilidad de hardware específico (GPUs / TPUs) que permite procesar algoritmos de gran complejidad en un periodo de tiempo muy reducido. Otra de las ventajas que aporta el DL frente a las técnicas de aprendizaje automático tradicionales es lo que se conoce como *Representation Learning,* o la capacidad de extraer las características intrínsecas de los datos de forma automática. Gracias al DL se han impulsado campos de la inteligencia artificial como el *Computer Vision,* o visión por computador, así como el *Natural Language Processing (NLP)* o procesamiento del lenguaje natural, ayudando a construir soluciones que hoy día conviven con las personas a través de nuestros ordenadores personales o dispositivos móviles.

Por tanto, podríamos definir la IA como aquel ecosistema donde encontramos diferentes tecnologías (ML, DL, etc.) que tienen en común el procesamiento de datos para obtener valor y conocimiento en base a unos objetivos predeterminados. Por eso encontramos definiciones según las que "la inteligencia artificial está en el centro de todas estas soluciones, en el punto donde todo converge"[18].

2. Convergencia de las tres tecnologías.

Hoy en día, toda conexión digital pasa a ser un origen de datos abriendo –con su masificación– un horizonte de detalles que nunca pudimos ver cuando estábamos limitados a las cantidades más pequeñas[19]. En el nuevo paradigma informacional y comunicacional que vivimos, los datos son la piedra angular de la sociedad del conocimiento, algo que en la vertiente productiva se manifiesta en la Cuarta Revolución Industrial o Industria 4.0. De hecho, la economía de los datos crece de tal manera que en la Unión Europa, la monetización de los datos podría duplicar sus valores en los cinco años siguientes a 2020[20].

El Big Data irrumpió con fuerza en nuestra sociedad gracias a la combinación de tres factores clave[21]. En primer lugar, el factor humano, comprendiendo tanto a las personas capacitadas para decidir y gestionar los algoritmos (*data scientist*) como personas que se dedican a estudiar el sector de negocio para implementar el proyecto de Big Data. En segundo lugar, encontraríamos los recursos tecnológicos (hardware y software) y finalmente, las fuentes de datos, las cuales cuentan con unas capacidades jamás vistas anteriormente.

Para analizar estas inmensas cantidades de datos han surgido un conjunto de técnicas que pertenecen al campo de la IA y reciben el nombre de "minería de datos"[22]. Es por lo que, estrechamente ligado al concepto de Big Data, encontramos el de Inteligencia Artificial (IA) que se nutre y necesita de grandes cantidades de datos y posibilita la explotación de esos macrodatos. Así, Inteligencia Artificial se configura como un nuevo

[18] LUCA, "¿Qué es la Inteligencia Artificial?", Diccionario Tecnológico. https://luca-d3.com/es/data-speaks/diccionario-tecnologico/inteligencia-artificial

[19] MAYER-SCHÖNBERGER, V., CUKIER, K., Big data. La revolución de los datos masivos, Madrid: Turner, 2013, pág. 22.

[20] IMREI, K. (Ed.), "Data as the Engine of Europe's Digital Future", The European Data Market Monitoring Tool Report, junio de 2019, pág. 53 http://datalandscape.eu/sites/default/files/report/EDM_D2.5_Second_Report_on_Policy_Conclusions_final_13.06.2019.pdf

[21] PÉREZ, C., "Aspectos legales del Big Data", Revista de Estadística y Sociedad, nº 68, 2016, p. 18.

[22] BARRIO, M. op. cit., p. 42.

factor de producción y no como un mero impulsor de la productividad[23], lo cual supondría una auténtica transformación del panorama existente hasta el momento.

Dos factores han sido clave para el desarrollo de la IA, el acceso ilimitado a la capacidad de procesamiento y el crecimiento del Big Data. Podríamos decir que "los datos son a la IA lo que la comida a los seres humanos" [24]. Y ese "alimento", entendido como Big Data, en gran medida es gracias a IoT, el cual puede considerarse como el "kilómetro cero" de esa enorme generación de datos. Esto mismo en retrospectiva: la ingente acumulación de información y el Big Data es lo que ha permitido en los últimos años que vaya haciéndose efectivo el desarrollo de la IA[25].

Otro elemento distintivo de la IA sería su capacidad autoaprendizaje, la cual marcaría la diferencia respecto a los avances tecnológicos de otras épocas[26]. Aquí entran en juego los ya mencionados conceptos de aprendizaje automático y aprendizaje profundo que precisamente diferencian estos sistemas de otros menos avanzados[27]. En este sentido, la IA tiene la capacidad de superar las limitaciones físicas del capital y el trabajo para abrir nuevas fuentes de valor y crecimiento.

Vemos, por tanto, cómo Internet de las Cosas, Big Data e Inteligencia Artificial –entre otros agentes claves de la nueva revolución industrial, como la robótica, la impresión 3D y 4D, la nanotecnología, la biotecnología y la ciencia de los materiales, entre otros, – son **realidades que difícilmente pueden entenderse por separado**. De hecho, gracias a IoT alimentamos los procesos de Big Data, cuyas soluciones se desarrollan y alcanzan el máximo esplendor con la IA.

Asimismo, la convergencia de las tres tecnologías cubre enfoques y técnicas conexas como *reinforcement learning*, ejemplo específico del *machine learning*; *machine reasoning* (que incluye la planificación, la programación, representación y razonamiento del conocimiento, búsqueda y optimización) y el conjunto de la robótica, que incluye el control, percepción, sensores y actuadores, así como la integración de todas las demás técnicas en los sistemas ciberfísicos.

Quedando establecida pues, la relación indivisible entre Inteligencia Artificial, Big Data e IoT, algunos autores señalan una nueva tecnología que viene a formar parte de esta ecuación: *Blockchain,* que proporciona un intercambio seguro de información entre entidades de una red distribuida y según se afirma[28], supondría una

[23] PURDY. M, DAUGHERTY, P., Informe "Inteligencia Artificial, el futuro del crecimiento", Accenture, 2016, p. 4. https://www.accenture.com/cl-es/insight-artificial-intelligence-future-growth

[24] PURDY. M, DAUGHERTY, P., Op. Cit., pág. 11.

[25] COTINO HUESO, L., "Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho", *Revista General de Derecho Administrativo*, nº50, 2019, p.7.

[26] CESE, "Inteligencia artificial: anticipar su impacto en el trabajo para garantizar una transición justa", Dictamen 2018/C 440/0, Comité Económico y Social Europeo, 6 de diciembre de 2018, p. 3.

[27] BEJERANO, P., "Diferencias entre machine learning y deep learning", Telefónica Think Big Empresas, 8 de febrero de 2017, https://blogthinkbig.com/diferencias-entre-machine-learning-y-deep-learning

[28] RABAH, K., "Convergence of AI, IoT, Big Data and Blockchain: A Review", The Lake Institute Journal, vol.1, núm.1, 2018, págs. 1-18.

expansión del concepto Big Data en cuanto a la visibilidad de las transacciones de datos entre todos los implicados.

En este contexto, la Unión Europea ha sido muy consciente desde un inicio de la importancia de los datos, y en particular, de la **economía de los datos**, pues ya en 2014 aprobó la Comunicación *Hacia una economía de los datos próspera* [29], para establecer las condiciones marco adecuadas para un mercado único de los macrodatos (*big data*) y la computación en nube, tratando de establecer las características de la futura economía de los datos. En esta línea, la Comisión Europea ha impulsado la denominada *economía de los datos*, en el contexto del **Mercado Único Digital**[30], cuya estrategia y hoja de ruta fue presentada en Mayo de 2015, a través de la Comunicación, *Una Estrategia para el Mercado Único Digital de Europa*[31]. Posteriormente, la Comisión Europea presentó en 2018 una estrategia de *Inteligencia artificial para Europa* [32], en cuyo marco se ha aprobado el Libro Blanco sobre Inteligencia Artificial[33] y la Comunicación *Una Estrategia Europea de Datos*[34] donde la Comisión afirma que "los datos son un recurso esencial para el crecimiento de la economía, la competitividad, la innovación, la creación de empleo y el progreso social en general". En junio de 2020 la Comisión aprobó una nueva Comunicación *El momento de Europa: reparar los daños y preparar el futuro para la próxima generación*[35] en la que el Mercado Único Digital se configura como una pieza fundamental en relación a la recuperación en torno a la COVID 19.

Aquí debemos traer a colación la Propuesta de Reglamento europeo relativo a la gobernanza europea de datos[36] cuyo objetivo es ampliar la disponibilidad de datos con miras a su utilización, mediante el aumento de la confianza en los intermediarios de datos y el refuerzo de los mecanismos para el intercambio de datos en el conjunto de la UE.

---

[29] COMISIÓN EUROPEA, "Hacia una economía de los datos próspera", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM/2014/0442 final, 2 de julio de 2014, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014DC0442&from=ES

[30] PARLAMENTO EUROPEO, "El mercado único digital omnipresente", Fichas temáticas sobre la Unión Europea Parlamento Europeo, https://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente

[31] COMISIÓN EUROPEA, "Una Estrategia para el Mercado Único Digital de Europa", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2015) 192 final, 6 de mayo de 2015, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=ES

[32] COMISIÓN EUROPEA, "Inteligencia artificial para Europa", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2018) 237 final, 25 de abril de 2018, https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF

[33] COMISIÓN EUROPEA, *Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*, COM(2020) 65 final, 19 de febrero de 2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

[34] COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 66 final, 19 de febrero de 2020, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&from=ES

[35] COMISIÓN EUROPEA , "*El momento de Europa: reparar los daños y preparar el futuro para la próxima generación*", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 456 final,

https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0456/COM_COM(2020)0456_ES.pdf

[36] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), COM(2020) 767 final https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0767&from=EN

3. Usos actuales de las tres tecnologías.

Las tres tecnologías tienen en común su inabarcable proyección hacia el futuro y las infinitas posibilidades de aplicación en cualquier ámbito de nuestra vida.

Actualmente, cabe destacar los siguientes casos de uso en los que se desarrollan, tanto en el sector privado como público:

- **Domotización y sensorización de hogares (domótica), edificios y ciudades,** para lograr mayores posibilidades, experiencias físicas, satisfacción y monitorización de los procesos. Cuando la sensorización se aplica a la infraestructura de núcleos urbanos para alcanzar la eficiencia hablamos de **Ciudades Inteligentes** (*Smart City*).
- **Movilidad, transporte, vehículos inteligentes en general y en particular, los coches autónomos,** siendo estos últimos según la DGT todos aquellos "con capacidad motriz equipados con tecnología que permita su manejo o conducción sin precisar la forma activa de control o supervisión de un conductor, tanto si dicha tecnología autónoma estuviera activada o desactivada de forma permanente o temporal"[37].
- **Drones** que se definen como "cualquier aeronave operada o diseñada para ser operada sin un piloto a bordo"[38].
- **Sensorización en procesos de fabricación industrial, comercio y consumo (B2B, M2M)** al conectar máquinas, piezas y sistemas creando redes inteligentes que se pueden controlar mutuamente y de manera autónoma, consiguiéndose todo ello a partir de los sistemas ciberfísicos y el denominado internet de los servicios[39].
- **Sensorización de dispositivos llevables o** "*wearables*", el conjunto de dispositivos electrónicos que llevamos como accesorios, incluyendo aquellas que a través de aplicaciones se emplean para indicaciones de salud. Es precisamente en el sector de la Salud en el que cobran especial relevancia las técnicas de Big Data e IA.
- **Prevención del fraude y blanqueo de capitales**

Del amplísimo espectro de aplicación, queda patente el poder de transformación que tienen estas tecnologías en la mejora de nuestras vidas, pudiendo apuntar otras de sus categorías sistemáticas como educación de calidad, transformación digital, cambio climático, desarrollo sostenible y ciberseguridad**.**

[37] DGT, "Instrucción 15/V-113 sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general", Dirección General de Tráfico del Ministerio del Interior, p. 1, http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/15.V-113-Vehiculos-Conduccion-automatizada.pdf

[38] COMISIÓN EUROPEA, *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea, y se deroga el Reglamento (CE)* nº 216/2008 del Parlamento Europeo y del Consejo, 2015/0277/COD, 7 de diciembre de 2015, artículo 3 (29).

[39] CEPAL, Informe "La Nueva Revolución Digital: de la Internet del consumo a la Internet de la producción". Comisión Económica para América Latina y el Caribe, 2018, p. 36, https://repositorio.cepal.org/bitstream/handle/11362/38604/4/S1600780_es.pdf

En relación con el mercado de las plataformas, según un Informe de IoT-Analytics[40] este se encuentra concentrado en unos pocos proveedores (plataformas genéricas), pero a la vez, tiende a la fragmentación (plataformas especializadas) y se encuentra en constante crecimiento.

Dentro de dicho mercado, según el Informe de IoT-Analytics encontramos 620 proveedores en 2019, lo que supone un incremento del 37% respecto al número de proveedores de 2016, cuantificado en 260.

Siguiendo el mencionado informe, si analizamos estos proveedores por sectores, encontramos que el sector de la fabricación y la industria ocupa el 50%, muy por delante de sectores como la Energía (34%), Movilidad (32%) y *Smart Cities* (31%). A continuación, le seguirían ámbitos como la salud, la cadena de suministro y el *retail*, quedando la agricultura (13%) casi a la par que la Administración pública (12%).

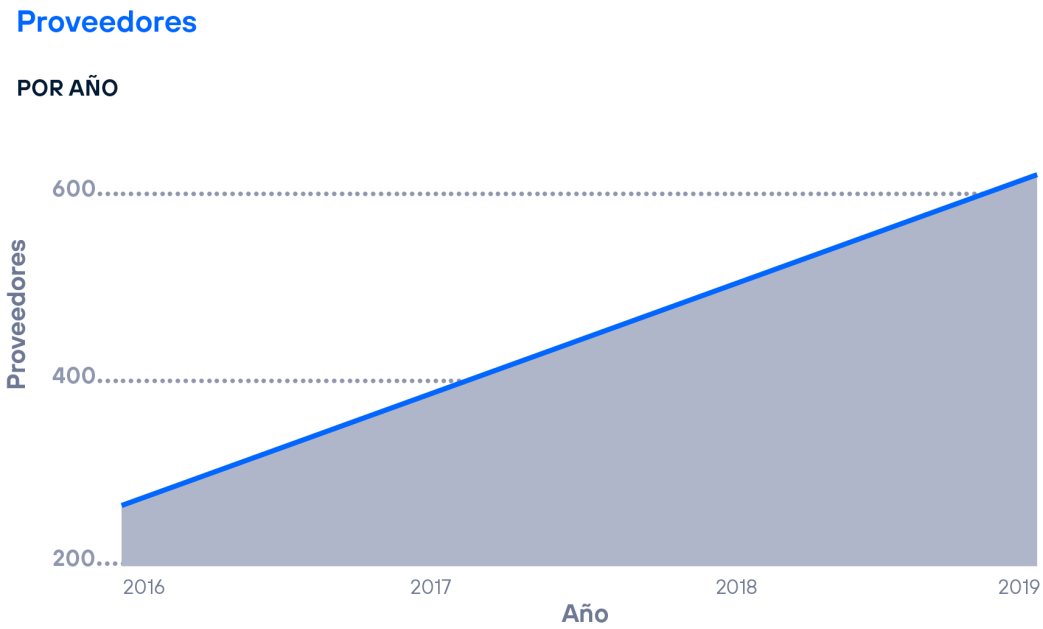

Figura 2: Evolución de proveedores por año. Elaboración propia.

[40] IoT ANALYTICS, IoT Platforms Company Landscape 2020, https://iot-analytics.com/product/iot-platforms-landscape-database-2020

Proveedores

POR SECTOR

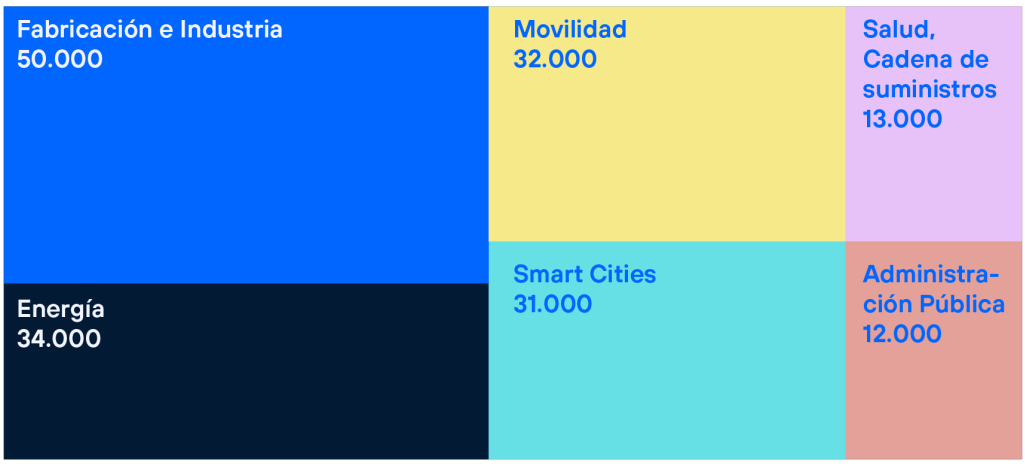

Figura 3: Proveedores por sectores. Elaboración propia.

Si atendemos al nivel de digitalización, como paso previo para la existencia y funcionamiento en la vida diaria de las personas de estas tecnologías, siguiendo el Informe de Fundación Telefónica[41], la banda ancha móvil ha experimentado un importante desarrollo en los últimos años y respecto a la banda ancha fija, más de la mitad de las subscripciones se realizan por cable o fibra óptica. En España, concretamente, el porcentaje de líneas de fibra óptica supera el 50%. Destaca el mencionado informe[42] que España, respecto al indicador de conectividad "es el país que mejor desempeño muestra dentro de las cinco principales economías de la Unión Europea".

[41] RODRÍGUEZ CANFRANC, P. et al., "Sociedad Digital en España 2019", Fundación Telefónica, abril 2020, pág. 28, https://www.fundaciontelefonica.com/noticias/informe-sociedad-digital-espana-2019

[42] Ibidem, pág. 29.

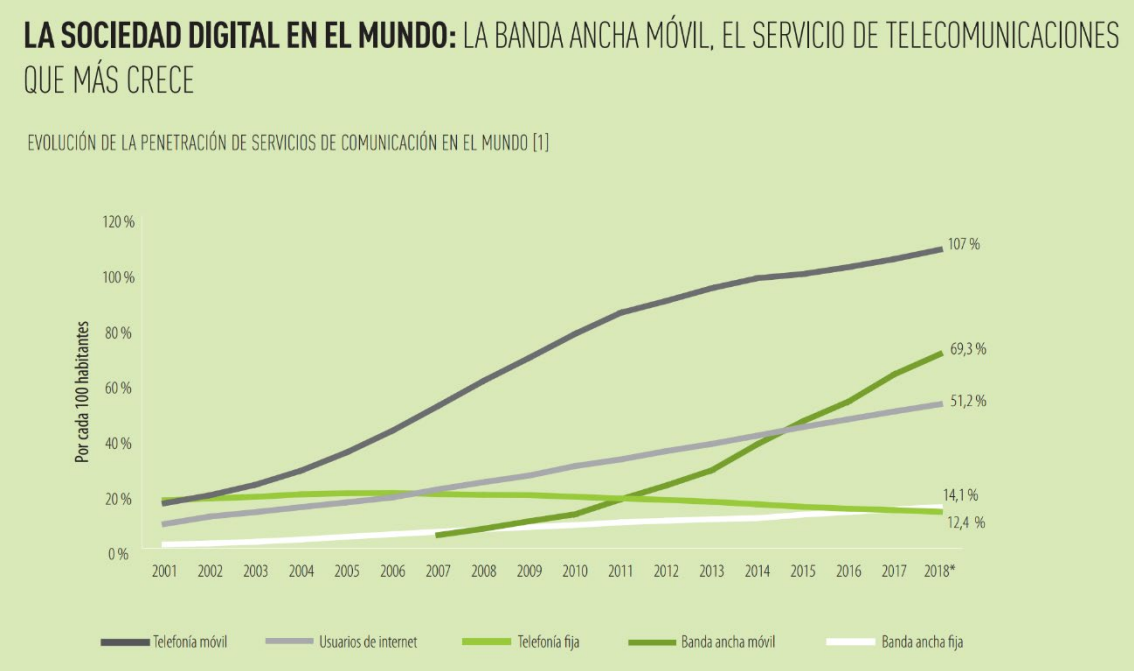

Figura 4: Evolución de la penetración de servicios de comunicación en el mundo. Fuente: Informe "Sociedad Digital en España 2019", Fundación Telefónica, pág. 27.

Por tanto, vemos cómo en España tenemos el sustrato perfecto para la implantación y desarrollo de estas tecnologías. A nivel de inversión, según la consultora IDC[43], España es el quinto país de Europa en inversión en IoT, solo por detrás de Alemania, el Reino Unido, Francia e Italia.

4. Gobierno del Dato (DG)

Se define Gobierno del Dato como el conjunto de roles y políticas que sirven para la correcta gestión de los datos dentro de una compañía, país, nación, comunidad, desde la definición de los sistemas origen, pasando por los procesos de negocio, procesos técnicos, hasta la seguridad y explotación de estos.

La Unión Europea, como primera medida de las anunciadas en el marco de la Estrategia Europea de Datos de 2020[44], ha presentado una propuesta de Reglamento europeo relativo a la gobernanza de datos ("Ley de

[43] IDC RESEARCH ESPAÑA, "El Mercado de Internet de las Cosas en España", https://idcspain.com/research/IoTSpain

[44] COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 66 final, 19 de febrero de 2020, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&from=ES

Gobernanza de Datos[45]") cuyo objetivo es crear un espacio común europeo de datos instaurando las condiciones necesarias para la puesta en común de datos en el mercado interior, mediante la creación de un marco armonizado para su intercambio y así, favorecer y propiciar la economía de los datos. Así, podemos ver la importancia del gobierno del dato también a efectos de cumplimiento normativo, pero que en último término y para cualquier organización va a permitir una gestión adecuada, eficiente, segura y de conformidad con los diferentes marcos normativos existentes que afecten a los datos (personales y no personales).

Se ha citado que los datos son "el alimento de la IA". El Gobierno del Dato asegura una buena calidad de estos alimentos, además de garantizar el origen y destino de los datos (quién los produce, quién los consume, a qué procesos se someten) y también es el medio técnico sobre el cual se implementa la regulación legal de accesos a los datos.

Los sistemas de tratamiento de datos tradicionalmente han venido implementando diferentes mecanismos técnicos de control, funcionando estos de forma independiente. La aportación del Gobierno del Dato es hacer de **orquestador** de estos y otros mecanismos, para lograr un **enfoque integral de la solución**, que abarca no solo a la parte **técnica** sino también a la **organizativa** y la **de negocio**.

Las nuevas tecnologías como el 5G, el Big Data o el IoT, enfocadas, por ejemplo, a la gestión de las infraestructuras (*Smart Cities*), dejan de manifiesto los enormes volúmenes de datos actuales y venideros.

Desde la Unión Europea se indica que el crecimiento de los datos desde 2018 a 2025 se espera que tendrá un **aumento de un 530%** (ver *European Data Strategy*[46]). Este crecimiento exponencial de datos debe ser gobernado para garantizar la ética, calidad, seguridad y otros muchos aspectos de este "gemelo digital".

Un concepto en boga ahora mismo es el de **gemelo digital**. Se refiere a la replicación de la vida cotidiana en los sistemas de información y aplica tanto a los procesos industriales como a las personas físicas. Esto abre la necesidad de disponer de mecanismos fuertes de Gobierno del Dato donde se vele por conceptos tales como la ética, la equidad y la seguridad aplicados a estos gemelos, ya que revierten sobre el mundo real.

Mientras un proceso industrial puede beneficiarse ampliamente de estos modelos, en su aplicación sobre las personas se debe extremar la precaución y cuidados, dada la sensibilidad de los datos tratados.

Otro de los temas candentes en la actualidad son los **fideicomisos o cooperativas** de datos, vinculados con los **espacios de datos** compartidos (concepto en contraposición a silos o datos duplicados). Estos espacios utilizan una serie de contratos entre partes por los que los titulares de los datos ceden de forma altruista sus datos para que sean tratados, con fines definidos por otras entidades (beneficiarios) pero manteniendo el control sobre los datos que generen. Este concepto lleva implícito una fuerte gestión en la seguridad, privacidad y normativa, en resumen, el gobierno efectivo de esos datos.

---

[45] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos, (Ley de Gobernanza de datos), COM(2020) 767 final https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[46] EUROPEAN UNION: Data Governance in Data Strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

Estos fideicomisos o cooperativas a veces son ejecutados en forma de ***Marketplace*** de datos con contratos implementados y securizados con ***Blockchain***, que garantizan la trazabilidad y unicidad del dato.

La Unión Europea en su Estrategia Europea de Datos[47] habla de la necesidad de estos espacios comunes relativos a:

- la industria (fabricación)
- Pacto Verde Europeo
- la movilidad
- la salud
- en materia financiera
- la energía
- sector agrario
- las administraciones públicas
- en materia de cualificaciones

Estos espacios deben velar por evitar sesgos y opacidad, y garantizar derechos y libertades, así como optimizar los diseños, todo con fines a la mejora de eficiencias y beneficios.

Sobre los espacios comunes es importante la aplicación del principio: "Datos tan abiertos como sea posible, tan seguros como sea necesario". Principios **FAIR** para la compartición y democratización de los datos:

F- *Findable*

A- *Accessible*

I- *Interoperable*

R- *Reusable*

A nivel nacional toda la estrategia europea y ley sobre gobierno del dato se capilariza en diferentes acciones y palancas plasmadas en el BOE[48], como son Agenda España Puede[49], ENIA[50], etc.

No queremos dejar de mencionar en este apartado uno de los pilares fundamentales sobre los que se asienta el Gobierno del Dato y que permiten la correcta gestión de la información, los metadatos.

Los metadatos son información de contexto que acompañan a los datos y permiten la aplicación de distintas disciplinas como la calidad, seguridad, organización, aspectos legales, ciclo de vida, integración de fuentes de dato.... muy relacionados con velar por los derechos de las personas tanto físicas como jurídicas.

---

[47] Op. Cit.

[48] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-10008

[49] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-Espa%C3%B1aDigital_2025.pdf

[50] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIAResumen2B.pdf

Parte 2: Impacto ético

El conjunto de tecnologías emergentes exploradas en el presente estudio, y muy especialmente la Inteligencia Artificial, abre la puerta a nuevas problemáticas de índole ética y por ello es necesario velar por el impacto de las posibles consecuencias en la vida de las personas impactadas por dichas tecnologías. Estas consecuencias no se habían presentado hasta ahora o, para mayor precisión, no se habían dado con la misma intensidad. Hablamos de sistemas que pueden incrementar las desigualdades sociales, cometer errores en sistemas vitales para las personas (ámbito de la justicia, recursos humanos), fomentar vicios en el comportamiento de los consumidores etc y en los que hay trabajar para que esto no ocurra.

Es por ello fundamental identificar dichos problemas y entender la forma en la que, desde diferentes organismos y empresas se están tratando, con el fin de construir sistemas basados en Inteligencia Artificial atendiendo a directrices éticas pensando en el bien común de la humanidad y no sólo en las funcionalidades u objetivos de negocio.

SESGOS

La consideración de los sesgos como uno de los principales riesgos de la IA es habitual en aquellos estudios o informes que especialmente se centran en la dimensión ética y jurídica de dicha tecnología. Sin embargo, como veremos, las distintas formas en las que se originan los sesgos hacen que deban abordarse no solo en el campo de la IA, sino también en los dispositivos IoT y en el contexto del Big Data.

L´*Autoritat Catalana de Protecció de Dades*, cita en su informe sobre la Inteligencia Artificial[51], la clasificación de distintos tipos de sesgos que lleva a cabo BAEZA-YATES, catedrático de Informática de la Universidad Pompeu Fabra y de la Northeastern University, que clasifica tres tipos de sesgos clásicos: el estadístico, el cultural y el cognitivo.

A grandes rasgos, el sesgo *estadístico*, según la clasificación anterior, procede del modo en el que obtenemos los datos, como por ejemplo, a través de los errores de medición en esta primera fase de obtención de información. Es evidente que gran parte del riesgo en la correlación de los dispositivos IoT, sistemas de Big Data e IA, recaería sobre los primeros, puesto que posibles errores de obtención de la información del dispositivo de IoT, podrían generar ese sesgo estadístico con el correspondiente impacto en el posterior proceso de tratamiento de información. El sesgo de tipo *cultural* está basado en concepciones de grupo como sociedad, por ejemplo, los estereotipos que pueden existir sobre un determinado grupo de personas por razón de su nacionalidad, género, religión o estatus social. Dichos sesgos impactan directamente en los resultados arrojados por los sistemas de inteligencia artificial, haciendo que la toma de decisiones incremente la desigualdad entre los grupos minoritarios o desfavorecidos. La inacción frente a este tipo de problemas en la IA, podría hacer que los nuevos datos que se generen por estos sistemas sigan adoleciendo de estos problemas discriminatorios, creando así un bucle de realimentación (*feedback loop*) negativo que hará que el problema siga persistiendo en la sociedad. Finalmente están los sesgos de tipo *cognitivo*, ya vinculados a nivel individual, que dependerán de las propias preferencias del individuo, convicciones, etc. Este último sesgo

[51] APDCAT, *Inteligencia Artificial: Decisiones Automatizadas en Cataluña,* 2020, pág. 21, https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf

puede ser especialmente útil para, una vez perfilado un individuo, suministrarle información destinada a gustarle a efectos de reafirmarse en sus propias convicciones y, en su caso, incluso suministrarle o generar *fake news* para dicho fin, para mantenerlo dentro de una suerte de filtro burbuja.

La materialización de dichos riesgos puede tener impactos fatales en los usuarios y ciudadanos y se trataría de un "lavado tecnológico" que haría creer que las decisiones algorítmicas son justas cuando en realidad están reproduciendo un sesgo entre la sociedad[52].

OPACIDAD

Se trata de un riesgo que, aunque afecta transversalmente a todos los sistemas de información, puede ser especialmente relevante en el contexto de estas nuevas tecnologías. El RGPD sitúa como uno de sus pilares, el principio de transparencia[53], siendo quizás uno de los aspectos que hoy es más fácilmente evaluable por parte de los titulares de los datos, ¿me están informando correctamente sobre las finalidades o bases legales cuando entrego mi curriculum en un portal de empleo? ¿Me informa de manera correcta esa aplicación sobre qué datos exactamente utiliza sobre mí para llevar a cabo sus funciones?

Dicho principio cobra un sentido aún más relevante y a su vez de una mayor complejidad, cuando nuestros datos son tratados para generar decisiones automatizadas sobre nosotros, más aún si cabe, si tales decisiones pueden tener consecuencias importantes en nuestros derechos y libertades. Dicha cuestión, no pasa desapercibida por el legislador europeo, al referirse a las decisiones automatizadas, en su considerando 71[54], cuando habla de los principios de lealtad y transparencia, y que sitúa también como un aspecto que debe ser informado a los interesados en cumplimiento de sus artículos 13 y 14. Dicha información, se refiere como mínimo a la "...información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado"[55].

---

[52] RICHARDSON, R., SCHULTZ, J., CRAWFORD, K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," 94 N.Y.U. L. Rev. Online, nº 192, marzo 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423

[53] N.B.:, Artículo 5 (Principios relativos al tratamiento) del RGPD: *"1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)"; Considerando (39): "...El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento."*

[54] N.B.: Considerando 71 del RGPD: "A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado *y se impidan, entre otras* cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas".

[55] N.B.: *RGPD en relación a los artículos 13.2 f) , 14.2 g) y 15.1 h).*

Sin embargo, la generalidad del término con la que se define la obligación de informar sobre esa automatización del tratamiento, puede plantear cuestiones jurídicas sobre el alcance de otros intereses en juego, puesto que una información totalmente detallada sobre el proceso del algoritmo o lógica que aplica un sistema de IA sobre una decisión, suponiendo que pudiera trasladarse de forma entendible para el ciudadano medio, podría estar revelando secretos comerciales o incluso procesos de *know how* susceptibles de protección jurídica, patentes o propiedad intelectual si aplicasen, poniendo en compromiso la totalidad o parte del modelo de negocio o estrategias de los distintos operadores económicos. Por otro lado, una información demasiado genérica, puede desnaturalizar el propio principio de transparencia y no aportar ningún tipo de información al ciudadano, contribuyendo a lo que se viene conociendo como efecto "caja negra" en el contexto de la IA.

El comentado efecto de caja negra, se utiliza por la Comisión Europea, en su "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica"[56], para ilustrar los posibles riesgos, especialmente en materia de responsabilidad civil cuando integramos IA con otros dispositivos, tales como los dispositivos IoT y no disponemos de suficiente información sobre el funcionamiento de cómo interacciona el sistema hasta la toma de decisiones final.

DERECHOS Y LIBERTADES

No es extraño por ello que, fruto de esos sesgos, los errores estadísticos, culturales y cognitivos que puedan afectar a las tres tecnologías comentadas, junto a la mayor o menor capacidad de decisión de dicho sistema que las integre, pueda impactar de manera relevante en los derechos y libertades de las personas que como ya vemos más claramente trascienden a la mera afectación del derecho de protección de datos y el derecho a la intimidad.

A efectos de llevar a cabo una primera aproximación sobre los derechos fundamentales afectados podríamos partir de un análisis de distintos textos, como puede ser nuestra Constitución, el Convenio Europeo de Derechos Humanos[57], la Declaración Universal de Derechos Humanos[58] o el Pacto Internacional de Derechos Civiles y Políticos[59]. También a efectos de dar una visión general, podemos destacar las observaciones del Libro Blanco de la IA en Europa[60], que dispone textualmente*:* " (...) El uso de la inteligencia artificial puede afectar a los valores sobre los que se fundamenta la UE y provocar la conculcación de derechos fundamentales, como la libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación

[56] COMISIÓN EUROPEA, "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica", Informe a la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, COM(2020) 64 final, 19 de febrero 2020, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064

[57] CONSEJO DE EUROPA, Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4 de noviembre de 1950.

[58] NACIONES UNIDAS, Declaración Universal de los Derechos Humanos, 217 (III) A. Paris, 1948.

[59] NACIONES UNIDAS, Pacto Internacional de Derechos Civiles y Políticos. Resolución 2200 A (XXI) de la Asamblea General, 16 de diciembre de 1966.

[60] COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial..., op. cit., pág. 13.

sexual, y, en su aplicación en determinados ámbitos, la protección de los datos personales y de la vida privada, el derecho a una tutela judicial efectiva y a un juicio justo, o la protección de los consumidores".

MEJORAR DISEÑOS

Si somos capaces de traducir una situación o problema en un modelo matemático con variables que pueden ser monitorizadas y pueden producir datos de salida, mediante algoritmos de Inteligencia Artificial podemos controlar y mejorar dicha situación o problema. Es decir, podemos enseñar al modelo en base a los resultados del pasado (a partir de los datos que ya tenemos), con el objetivo de realizar predicciones presentando nuevos datos de entrada.

Existen multitud de aplicaciones que representan ejemplos de Inteligencia Artificial saludable que no tiene efectos perjudiciales para las personas. Uno de ellos es la metodología *Moneyball*[61] desarrollada en 2001 por el entrenador de béisbol de los Oakland Athletic Billy Beane. Mediante técnicas innovadoras de analítica y predicción, él y sus colaboradores construyeron un equipo de bajo presupuesto que debía competir con equipos mucho más importantes. Estas técnicas, que sólo ellos usaban en ese momento, mostraron que las decisiones que hasta ese momento se tomaban en el mundo del béisbol eran engañosas e incluso irracionales. Con esta información cambiaron la estrategia y centraron la selección de jugadores en aquellos procedentes de las ligas universitarias en lugar de contratar a jugadores más veteranos cuyas nóminas eran muy altas. Como consecuencia de este tipo de decisiones Billy Beane llevó a su equipo hasta las finales de ese año, pasando por delante de equipos con un presupuesto mucho mayor.

Moneyball representa un uso saludable[62] de la Inteligencia Artificial porque sigue los siguientes principios:

- Es un modelo transparente que cualquiera puede entender y los datos de entrenamiento de los algoritmos están disponibles para todo el mundo[63].
- Tiene rigor estadístico: los científicos de datos tienen a su disposición un inmenso catálogo de datos de entrenamiento, y dichos datos son *relevantes* para los resultados que se están intentando predecir.
- Los datos están siendo actualizados diariamente por fans de todo el mundo, de manera que los científicos pueden comparar los resultados con las predicciones realizadas por sus modelos y ver dónde han fallado.

No todas las aplicaciones basadas en Inteligencia Artificial siguen estos principios y muchas de ellas no tienen el mismo rigor a la hora de seleccionar los datos de entrenamiento para que sean masivos y relevantes, lo que lleva a situaciones de sesgo que pueden tener serias consecuencias para las personas afectadas.

[61] N.B.: *vid. Moneyball: The Art of Winning an Unfair Game, autor Michael Lewis, 2003.*

[62] Cathy O'Neil afirma que "El béisbol es un caso práctico sin efectos perniciosos y nos servirá de ejemplo positivo con el que comparar los modelos tóxicos o ADM que están aflorando en tantísimas áreas de nuestra vida". O'Neil, C., Armas de destrucción matemática, Ed. Capitán Swing, 2017, p.27.

[63] N.B.: Los datos de los partidos de béisbol han sido recogidos desde hace más de 100 años por fans de este deporte, y están disponibles a través de diferentes webs como https://sabr.org/how-to/statistical-databases-and-websites

Un ejemplo de ello es la herramienta COMPAS, usada por la justicia americana para analizar el riesgo de reincidencia de un convicto. Jueces de todo el país se apoyan en ella para tomar decisiones acerca del futuro de los presos. Esta herramienta, basada en la respuesta de los convictos a una evaluación de 137 preguntas causó polémica al descubrirse en 2014 que introducía un sesgo racista. Si bien las predicciones eran correctas en un gran porcentaje (clasificaba correctamente una persona que podía llegar a reincidir o no), cuando se producían errores éstos se daban principalmente en personas de raza negra y en mucha menor medida en las personas de raza blanca[64]. Cuando se descubrió dicho comportamiento, la empresa encargada de la solución se negó a revelar el detalle del algoritmo alegando problemas de competencia. A pesar de las críticas recibidas, se sigue usando esta herramienta con restricciones (se deja claro que se trata de una caja negra, que hay dudas acerca de la validez de los resultados, que no debe en ningún caso sustituir el juicio de un humano, que debe ser constantemente monitorizada...).

Otro ejemplo de aplicación basada en Inteligencia Artificial con impacto negativo para las personas es el caso de TAY, el chatbot diseñado para imitar los patrones de lenguaje de una adolescente estadounidense de 19 años, que fue lanzado el 23 de marzo de 2016. Aparte de proveer un entrenamiento inicial, se dejó abierta la posibilidad de que el chatbot siguiera aprendiendo a través de las primeras interacciones con usuarios humanos de Twitter. El resultado fue que, al cabo de unas pocas horas, el chatbot respondía a los mensajes de otros usuarios con comentarios que contenían una gran carga sexual y racista. Tras varios intentos de contener la situación, se decidió cerrar la cuenta asociada al chatbot tras sólo 16 horas de su puesta en funcionamiento[65]. Diferentes investigadores explicaron que este comportamiento fue comprensible en la medida que no se habían definido cuáles eran los comportamientos inapropiados.

Lo anterior son ejemplos de implementaciones de Inteligencia Artificial que si no se revisan con minuciosidad pueden provocar consecuencias negativas en las personas. La razón principal, si comparamos su implementación a la de la metodología *Moneyball*, se debe a que los datos de entrenamiento que han sido usados son mucho más limitados (en COMPAS se han basado en entrevistas de pocas preguntas, en TAY los datos han sido mensajes principalmente de Trolls de Twitter, ...) y que el modelo es deficiente en términos de transparencia, siendo imposible saber por qué se han tomado determinadas decisiones. El libro *Weapons of Math Destruction*[66] de Cathy O'Neil recopila un gran número de ejemplos de IA que desde hace tiempo resultan relevantes en la vida de las personas (evaluación de desempeño en el puesto de trabajo, precio de seguros etc), especialmente en la sociedad americana.

[64] THE GUARDIAN, "Rise of the racist robots – how AI is learning all our worst impulses", por Stephen Buranyi, 8 de agosto de 2017, https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html>.

[65] https://www.xataka.com/robotica-e-ia/microsoft-retira-su-bot-de-ia-despues-de-que-este-aprendiera-y-publicara-mensajes-racistas

[66] O'Neil, C., *Armas de destrucción matemática*, Ed. Capitán Swing, 2017.

Parte 3: Impactos legales

1. Los derechos fundamentales en la sociedad digital.

La protección de datos personales es un derecho fundamental que no se reduce a aquellos datos más íntimos, sino que se proyecta sobre cualquier tipo de dato personal, sea íntimo o no. Es decir, "todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo" (Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre)".

A la hora de realizar cualquier operación que implique un tratamiento de datos de carácter personal, deberán observarse los requerimientos derivados de la legislación en materia de protección de datos de carácter personal.

El desarrollo e integración de las tecnologías de IoT, Big data e Inteligencia Artificial, constituyen una realidad innegable para las empresas y requieren como presupuesto una **libre circulación de datos**, sean personales o no. Es por ello que se aprobó el Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea[67], siendo de plena aplicación desde Mayo de 2019.

Ambas normas, responden a la necesidad de crear un marco político y jurídico claro, adaptado para la economía de datos, suprimiendo las barreras que subsisten a la circulación de datos y abordando las incertidumbres jurídicas creadas por las nuevas tecnologías basadas en datos, tal y como plasmó la Comisión Europea en su Comunicación *Construyendo una economía europea de datos*[68]. De hecho, así lo señala el Considerando 13 del Reglamento, cuando afirma que "el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales"[69].

El debate sobre los derechos humanos en las TIC suele ser monopolizado por la intimidad y la protección de datos; sin embargo, conviene recordar que nuestra Constitución, reconoce otros derechos fundamentales que se protegen al más alto nivel. No obstante, incluso en el marco de tales derechos fundamentales situados en un mismo espacio sistemático de la Constitución, en situaciones de conflicto entre los mismos, existen intensidades variables, que se deducen de sus límites intrínsecos y extrínsecos. Es claro cuando estamos ante una colisión entre el derecho a la vida vs derecho a la privacidad, pero hay otros supuestos en los que se produce colisión y hay que ponderar, por ejemplo, cuando entran en colisión el derecho a la libertad de información y a la intimidad. En este sentido, la STC 24/2019, de 25 de febrero, nos recuerda su doctrina en los supuestos de colisión entre el derecho a la libertad de información y a la intimidad, señalando que: "En la

[67] LOZA CORERA, M., "Hacia la economía de los datos europea: nuevo reglamento europeo 2018/1807", Govertis Advisory Services, 10 de diciembre de 2018, https://www.govertis.com/hacia-la-economia-de-los-datos-europea-nuevo-reglamento-europeo-2018-1807#_ftn3

[68] COMISIÓN EUROPEA, "La construcción de una economía de los datos europea", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM (2017) 9 final, 10 de enero de 2017.

[69] Op. Cit., AEPD, *Código de buenas prácticas....*

relación con este último derecho fundamental a la intimidad, este Tribunal ha venido entendiendo que la relevancia pública de la información justifica la exigencia de que se asuman perturbaciones o molestias ocasionadas por la difusión de una determinada noticia"[70].

Por ello, reafirmamos que el debate no debe agotarse en la afectación a la intimidad y protección de datos, sino también a los restantes derechos fundamentales en juego, como se observa del propio Reglamento General de Protección de Datos que reitera de forma finalista, la necesidad de proteger los *derechos y libertades fundamentales* de las personas más allá de la estricta protección de sus datos personales. Dicho enfoque centrado en la persona se define también en el contexto de la IA, como antropocéntrico que ha reconocido la Comisión Europea[71] y debe irradiarse a los sistemas que le sirvan para alcanzar su finalidad, esto es, los dispositivos IoT y los sistemas de Big Data.

Es por ello que no solo debemos tener en cuenta los riesgos respecto a la privacidad sino también riesgos referidos a la propia seguridad personal y a posibles daños personales, además de los físicos a nuestra propiedad. Por ejemplo, según recientes análisis de vulnerabilidad en productos para el hogar inteligente, atacantes podrían desbloquear puertas y candados de IoT, cambiar las temperaturas del termostato inteligente más allá de los máximos de fábrica, etc..por lo que hay que trabajar desde el diseño de estas soluciones para evitar que esto ocurra[72].

En el contexto del desarrollo de las tres tecnologías comentadas, en la medida en que las mismas integran un sistema cuyo objetivo es gestionar de manera inteligente una tarea u objetivo, en muchas ocasiones las consideraciones sobre los riesgos, dadas las dependencias que se generen entre sí, obligan a llevar a cabo una **consideración global de los riesgos**[73]. A título de ejemplo, como ya advertíamos cuando hablamos de los sesgos, los defectos en los sesgos en la toma de decisiones de un sistema de inteligencia artificial, pueden no traer causa directa de los algoritmos o lógicas aplicados, sino de los propios datos recogidos a través de dispositivos IoT quizá de forma defectuosa o con un sesgo determinado, y dichos sesgos son precisamente amplificados al tratarse con técnicas de Big Data, originando por tanto un sesgo en la decisión final del sistema

[70] TRIBUNAL CONSTITUCIONAL, Sentencia 24/2019, de 25 de febrero, FJ 5, http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25869#complete_resolucion&fundamentos

[71] COMISIÓN EUROPEA, Directrices éticas para una IA fiable, Grupo de expertos de alto nivel en Inteligencia Artificial, abril de 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[72] TSCHIDER, Ch., "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence", *96 Denv. U. L. Rev. 87 Age*, marzo de 2018, pág. 120.

[73] COMISIÓN EUROPEA, "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica"..., op. cit.

N.B.: "...Otros riesgos adicionales que pueden afectar a la seguridad son los derivados de la complejidad de los productos y los sistemas, ya que una serie de componentes, dispositivos y productos pueden integrarse e influir en el funcionamiento de los otros (p. ej., productos que forman parte de un ecosistema doméstico inteligente). Esta complejidad ya se trata en el marco jurídico de la Unión en materia de seguridad (...). En concreto, cuando el productor lleve a cabo la evaluación del riesgo del producto, debe considerar el uso previsto, el uso previsible y, en su caso, el mal uso razonablemente previsible. Por ello, si el productor prevé que su dispositivo estará interconectado e interactuará con otros dispositivos, debe considerar estos aspectos en la evaluación del riesgo. Los usos o malos usos se determinan sobre la base, por ejemplo, de la experiencia de usos pasados del mismo tipo de producto, las investigaciones de accidentes o el comportamiento humano. La complejidad de los sistemas también se trata más específicamente en la normativa sectorial de seguridad, como el Reglamento sobre los productos sanitarios y, en cierto grado, la Directiva relativa a la seguridad general de los productos. Por ejemplo, el productor de un dispositivo conectado, destinado a formar parte de un ecosistema doméstico inteligente, debe poder prever razonablemente que sus productos tendrán un efecto en la seguridad de otros productos (...)".

de la IA. De hecho, según indica la Comisión Europea, existen riesgos incrementados por razón de la complejidad de los productos y servicios cuando se interrelacionan con otros, como por ejemplo, en el contexto de productos para nuestro hogar inteligente, el diseño de la IA que gestiona el hogar no solo debe tener en cuenta sus propios riesgos de funcionamiento sino que deberá tener en cuenta los riesgos de integración de otros productos, en este concreto ejemplo, claramente los dispositivos de IoT que eventualmente puedan conectarse en el sistema de gestión inteligente de nuestro hogar[74].

Si bien es cierto que, tal como se ha expuesto en el presente informe, los avances en IA, junto a Big Data e IoT, son especialmente prometedores en el campo de la Salud y el Bienestar del individuo, existen también situaciones de riesgo que se deben tener en cuenta para evitar un impacto perjudicial en los derechos fundamentales, como pueden ser discriminaciones indebidas por razón de salud del individuo, especialmente graves si nos encontramos en contextos de eventuales pandemias globales como la vivida por causa de la COVID19 o la exclusión sesgada de individuos, por ejemplo, al contratar un seguro de vida o de salud.

Más relacionado con el campo del **derecho a la vida** en sentido más estricto, la existencia de aplicaciones militares que, mediante sistemas de IA, seleccionan y ejecutan sin intervención humana objetivos humanos, a través de las conocidas LAWS (*Lethal Autonomous Weapons*), han puestos de manifiesto conflictos éticos por parte de la Comisión[75] y el Parlamento Europeo[76].

La Comisión Europea también se ha pronunciado respecto de la seguridad en la producción de los sistemas de IA, IoT y robótica, indicando que, pese a que gran parte de la legislación, tanto general como sectorial, fue aprobada antes de que tales tecnologías fueran emergentes[77], el marco regulatorio en materia de seguridad de los productos es tecnológicamente neutro, por lo que no puede excluirse la aplicación del marco de seguridad de los productos, pero, no obstante, respecto a los marcos legislativos en materia de responsabilidad civil, resulta esencial que se incorporen dichas tecnologías.

Respecto al derecho fundamental **de igualdad y no discriminación**, debemos tener en cuenta que el derecho de igualdad se trata de un derecho genérico, que se hace valer en el contexto de otros derechos. Por otro lado, conviene recordar que la forma en que se produce la discriminación puede ser directa o indirecta. La discriminación directa, obedece a un trato desfavorable hacia una persona, por razón de raza, sexo, orientación sexual, identidad de género u otros motivos de carácter personal o social. La discriminación indirecta, se basa en disposiciones, criterios o prácticas aparentemente neutras que pueden ocasionar un trato desfavorable hacia una persona, por razón de raza, sexo, orientación sexual, identidad de género u otros motivos de carácter personal o social.

Si bien es cierto que una instrucción o sistema de evaluación de un algoritmo que incluya una discriminación racial de carácter directa puede resultar obvia , distintas autoridades e informes, han puesto de manifiesto que el verdadero riesgo en este sentido es precisamente que a través de los sesgos, se generen supuestos de discriminación indirecta ya sea porque los datos se recogen de fuentes que ya han sido elaboradas o

[74] Ibidem.

[75] COMISIÓN EUROPEA, Ethics Guidelines for Trustworthy AI (draft), op. cit.

[76] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 12 de septiembre de 2018, sobre los sistemas armamentísticos autónomos, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_ES.html

construidas en base a un sesgo ya existente o porque se establece una discriminación sobre un parámetro que aparentemente no es racista o sexista, pero que su incidencia afecta a un porcentaje extremadamente alto de un determinado grupo étnico, racial o de género, provocando a efectos prácticos una discriminación en perjuicio de dicho grupo[78].

En relación al derecho de **libertad de expresión**, son conocidos en la actualidad los distintos sistemas preventivos que las plataformas para compartir contenido utilizan, por ejemplo, para evitar que se infrinjan los términos y condiciones de sus servicios. Sobre dichos sistemas, si bien existe cierta aceptación social en cuanto que pueden prevenir determinadas acciones que a nivel internacional son comúnmente consideradas como reprochables, como puede ser la pornografía infantil o el enaltecimiento de acciones terroristas, no es menos cierto que existen sistemas preventivos de filtrado que han suscitado mayor controversia, como las relacionadas con las plataformas de creación de contenido y la existencia de algoritmos y sistemas de detección de obras de usuarios que puedan infringir derechos de propiedad intelectual de terceros. La cuestión sobre esta capacidad cada vez mayor de sistemas de IA que sean capaces de filtrar preventivamente el contenido que puede ser "subido" a la red, plantea sin duda cuestiones jurídicas sobre el alcance del concepto de "censura previa", prohibida por nuestra Constitución[79].

En cuanto al **derecho a la libertad de información**, como sujetos pasivos, ya ha sido advertido a nivel institucional, sobre el riesgo de entrar en cámaras de eco o como comentábamos en relación a los sesgos, los filtros burbuja[80]. La personalización cada vez más detallada del perfil de usuario que usan los servicios de los buscadores, puede provocar que el usuario solo reciba la información que el sistema de IA entiende que le gustará, de conformidad con los patrones manifestados por este o incluso de conformidad con los intereses de terceros que puedan influenciar en la gestión de los distintos algoritmos que utilicen los buscadores.

En relación al **derecho a elecciones libres, sistemas políticos democráticos** ¿pueden considerarse elecciones libres, aquellas donde se manipulen las percepciones de los votantes, a efectos de que voten en un sentido u otro? Cabría quizás antes definir en qué punto podemos hablar de captación de voto, campaña electoral o directamente de manipulación.

En este aspecto, cobra especial importancia a efectos de una posible manipulación, los comentados sesgos cognitivos, que pueden potenciarse, por ejemplo, en el campo de la política, mediante sistemas de Big Data que perfilen grandes volúmenes de votantes y segmentos ideológicos[81] a través de sus interacciones en las redes sociales y mediante otras herramientas de IA, como por ejemplo la generación automatizada y cada vez con mayor capacidad para engaño de *fake news*, *Deep Fakes*, Bots u otros mecanismos, para dirigir mensajes

[78] EL PAÍS, "Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres", por Isabel Rubio, 12 de octubre de 2018, https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html

[79] ESPAÑA, Constitución Española, BOE 29 de diciembre de 1978, artículo 55.

[80] CONSEJO DE EUROPA, "Algorithms and human rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications", Committee of experts on internet intermediaries (MSI-NET), 2018, https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

[81] TRIBUNAL CONSTITUCIONAL, Declaración inconstitucionalidad artículo 58bis LOPDGDD, vid. SENTENCIA 76/2019, de 22 de mayo, https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf

y campañas de marketing político cada vez más personalizadas y perfeccionadas, dejando en un segundo plano la idoneidad del candidato o propuesta política y apostando por sistemas de marketing especialmente agresivos[82]. Como podemos observar, el impacto ya no solo se sitúa en el contexto de la libertad de información, sino que impacta directamente sobre el propio sistema democrático[83] con especial vulnerabilidad para aquellos sistemas de elección directa (procesos consultivos o referéndums, sistemas de elección directa del candidato, etc.).

2. Concreción de los riesgos en materia de privacidad

En materia de protección de datos personales, los requerimientos normativos derivan del **Reglamento 679/2016 General de Protección de Datos**, en adelante RGPD, complementado en el caso nacional, por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el cual parte de la premisa[84] de que la protección de datos no puede ser un obstáculo para el buen funcionamiento del mercado interior y todo ello sin ceder en los estándares de protección para garantizar este derecho:

"La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales". [85]

En relación con el RGPD, destacamos el **consentimiento**, **transparencia** y **limitación de la finalidad** en el tratamiento de los datos de carácter personal.

Tanto el RGPD como la conocida **propuesta de Reglamento ePrivacy**[86], establecen las máximas garantías para la obtención del consentimiento[87] libre del usuario y la transparencia[88] sobre el tratamiento de nuestra información en comunicaciones electrónicas. Tampoco debe descuidarse que la finalidad debe limitarse a la

[82] N.B.: Puede citarse también el conocido caso de Cambridge Analytica, vid. https://www.xataka.com/privacidad/el-escandalo-de-cambridge-analytica-resume-todo-lo-que-esta-terriblemente-mal-con-facebook

[83] THE GUARDIAN, "The great British Brexit robbery: how our democracy was hijacked", por Carole Cadwalladr, 7 de mayo de 2017, https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

[84] N.B.: *En el considerando 13 RGPD se dice así: "El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".*

[85] MERCADER UGUINA, J. R., "El futuro del trabajo y el empleo en la era de la digitalización y la robótica", En: DE LA QUADRA-SALCEDO, T., PIÑAR MAÑANAS, J. L. (Dirs.), Sociedad digital y Derecho, Madrid: BOE, 2018, pág. 617,

https://www.boe.es/publicaciones/biblioteca_juridica/abrir_pdf.php?id=PUB-NT-2018-97

[86] COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), 2017/0003(COD), 10 de enero de 2017, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

[87] N.B.: vid artículos 7 y 8 RGPD, y 9 Reglamento ePrivacy.

[88] N.B.: vid artículos 13, 14 RGPD y artículo 10 Reglamento ePrivacy.

proyectada al tratamiento y debidamente informada al usuario, entre otros extremos, requiera o no dicho tratamiento su consentimiento.

BIG DATA

La afectación de los derechos a la privacidad en el campo del Big Data es clara. En primer lugar, debe cumplirse con el deber de información y, para el caso de requerir consentimiento como base de legitimación, su adecuada obtención y gestión para con el interesado, por lo que la transparencia ocupa un lugar esencial, no siempre fácil de articular de forma operativa si tenemos en cuenta el alto volumen de interesados que potencialmente puede alimentar el sistema de Big Data. Señala la AEPD que un posible riesgo legal puede ser el uso posterior de los datos adquiridos para una finalidad determinada, que luego son reutilizados para otra de la cual el titular de los datos no fue informado.

Asimismo, la generación de perfiles o *profiling*, puede determinarse como uno de los principales riesgos asociados a dicha tecnología tal como señala la AEPD[89]. Un riesgo que entendemos, no sólo es relativo a la simple generación de perfiles, sino también a que la tipología de perfiles pueda utilizarse en modelos de predicción, o incluso en sistemas de IA. Ulteriormente generarían discriminaciones o introducirían sesgos perjudiciales para determinados grupos de poblaciones con el agravante de que se traten de grupos especialmente vulnerables.

Otro elemento a considerar es la distinta procedencia de los datos de distintas fuentes, con una mayor complejidad de actores intervinientes en el proceso, y por ello la existencia de responsables del tratamiento, corresponsables y/o encargados del tratamiento, cuyas relaciones deberán regularse debidamente y asegurarse, especialmente el responsable de los datos, de que elige diligentemente al correspondiente proveedor o socio para el tratamiento de tales datos y de que estos últimos actúen con la debida diligencia. Serán claves también las previsiones relativas a la conservación y reutilización de los datos.

INTERNET DE LAS COSAS

Los retos en materia de protección de datos de carácter personal dentro del sector del Internet de las Cosas ya fueron puestos de manifiesto por el Grupo de Trabajo del artículo 29[90] y consisten en articular los correctos mecanismos para que los usuarios de este tipo de servicios mantengan bajo su completo control sus datos de carácter personal, a lo largo de todo el ciclo de vida del producto o servicio, mediando siempre un consentimiento informado, libre y específico. Es por ello que el derecho a la protección de datos es el primer impactado por esta tecnología.

La tecnología IoT se basa en proporcionar servicios que suponen una alta penetración en la vida de las personas al captar una gran cantidad de datos que puede tener un carácter altamente sensible. La interacción

[89] AEPD, *Código de buenas prácticas..., op. cit.*

[90] GT29, Dictamen 8/2014..., op. cit.

multilateral de las conexiones genera un flujo de datos complejo que difícilmente se puede manejar con las herramientas de usuario.[91]

Además, la complejidad propia de este tipo de servicios puede implicar que la comunicación entre los distintos objetos implicados en el Internet de las Cosas sea activada de una forma automática y por defecto, sin que el usuario sea consciente de dicho hecho. En esencia es necesario proteger al usuario para que en la interactuación de los objetos pueda definir cómo quiere controlar el flujo de datos generado. En este sentido, si no se es capaz de controlar ese flujo en su primer estadio, difícilmente el usuario podrá controlar los estadios posteriores en donde los datos son tratados fuera de su área de influencia y en donde además, se puede interactuar con otros avances tecnológicos como pueden ser el *Cloud Computing* o el *Big Data*[92].

INTELIGENCIA ARTIFICIAL

En el ámbito relativo a la IA, dado que es necesario el tratamiento de grandes cantidades de datos, aplican los riesgos para la privacidad mencionados en los apartados anteriores relativos a *Big Data* e IoT.

Tal y como afirma la AEPD[93], "el que toma la decisión de realizar el tratamiento es responsable y no puede escudarse en la carencia de información o el desconocimiento técnico para evadir su responsabilidad a la hora de auditar y decidir la adecuación del sistema". Es por ello que resulta imprescindible que, antes de poner en marcha una solución basada en IA, se adopten las medidas necesarias en materia de privacidad desde el diseño y por defecto se lleven a cabo las correspondientes Evaluaciones de Impacto en Protección de Datos o, en su caso, Análisis de Riesgos. Como también afirma[94] la AEPD "lo que en ningún caso resulta aceptable es trasladar la responsabilidad al propio sistema IA".

Será por tanto imprescindible cumplir con el deber de transparencia e información para con el interesado e informarle, en el caso de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 22, apartados 1 y 4 del RGPD, y al menos en tales casos, de que es información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

[91] SANTAMARÍA RAMOS, F. J.: "Internet de las cosas: un desafío para la protección de datos personales", Actualidad Administrativa nº 7-8, julio-agosto 2015, págs. 40-57.

[92] Ibidem.

[93] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial..., op. cit., pág. 19.

[94] Ibídem.

PARTE 4: Impactos tecnológicos.

1. Visión general de los riesgos.

Desde 2006 el *World Economic Forum* presenta anualmente el documento "Informe Global de Riesgos"[95] en el que recoge los principales riesgos que se deben afrontar a nivel mundial, clasificados según su probabilidad e impacto. Los riesgos tecnológicos relacionados con la seguridad de la información ya aparecían en las primeras ediciones del informe, pero fue en el informe del año 2012 cuando se definió el riesgo de ciberataques, situándose entonces a la cabeza en cuanto a probabilidad de materializarse.

En el informe de 2020, el *World Economic Forum* reitera la necesidad de crear una fuerte cultura de la ciberseguridad y en el informe de 2021[96] los fallos en ciberseguridad engrosan la lista de los riesgos más probables de causar un impacto negativo en los próximos diez años. El volumen de datos tratados será cada vez mayor y crecerá a gran velocidad con la generalización de tecnologías disruptivas como *blockchain*, la computación cuántica, la conectividad ubicua (que surgirá con el despliegue de 5G) o las necesidades que surjan con la consolidación de la nueva revolución industrial. Del mismo modo que estas nuevas tecnologías apoyarán el progreso socioeconómico, el riesgo a ciberataques para cada uno de estos nuevos escenarios aumentará en frecuencia y en impacto.

En este contexto, la ciberseguridad debe, además de prevenir las amenazas internas y externas, ser capaz de detectar los ataques en tiempo real para darles una respuesta rápida y adecuada con el objetivo de minimizar los daños.

La adopción de soluciones innovadoras tecnológicamente basadas en tecnologías denominadas disruptivas conlleva nuevos riesgos de seguridad derivados de la falta de madurez de las medidas de protección.

Con el despliegue masivo de dispositivos IoT, tanto a nivel empresarial como doméstico, la superficie de exposición aumenta considerablemente. Esto implica que el perímetro a proteger sea cada vez mayor, hasta el punto de convertirse en el propio dispositivo: mayor número de activos, aumento –en número y extensión– de las redes inalámbricas, y con protocolos diversos (*Bluetooth*[97], LoRa[98], NB-IoT[99], SigFox[100], etc.), lo que hace especialmente importante la necesidad de adoptar estrategias de seguridad desde el diseño y la seguridad por defecto. Asimismo, esta desaparición del concepto de perímetro como zona confiable, ha hecho que las medidas de prevención, que eran las predominantes en las estrategias de ciberseguridad de

[95] WEF, "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications", 2020, https://www.weforum.org/global-risks/reports

[96] World Economic Forum, *The Global Risks Report 2021*, 16th Edition, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[97] N.B.: Tecnología de acceso inalámbrico para la transmisión de datos por radiofrecuencia entre aparatos.

[98] N.B.: Tecnología inalámbrica que emplea un tipo de radiofrecuencia patentado por Semtech; como tipo de comunicación, encuentra usos militares y espaciales.

[99] N.B.: Narrowband-IoT es una tecnología útil para objetos cotidianos que requieren pequeñas cantidades de datos en períodos de tiempo largos.

[100] N.B.: Se trata de otra tecnología de conectividad en Internet de los objetos.

hace unos años, hayan ido cediendo protagonismo a medidas basadas en la detección, respuesta y recuperación ante incidentes.

Al igual que sucede con Big Data, la Inteligencia Artificial, introduce riesgos de seguridad y privacidad asociados al tratamiento masivo de datos y a las herramientas de análisis de los mismos. La IA juega también un papel activo en materia de seguridad, ya que puede utilizarse en aplicaciones de detección y respuesta de ciberataques o en el caso opuesto, como una aliada de los ciberatacantes. No es novedad[101] que el cibercrimen adopta los avances en inteligencia artificial y automatización para comercializar nuevas amenazas con las que atacar infraestructuras críticas. En este sentido, existe una carrera tecnológica en ambos lados para desarrollar las mejores soluciones y productos. Los cibercriminales tienen a su alcance numerosos recursos lo que hace que la variedad y complejidad de las amenazas que se benefician de esta tecnología aumente enormemente.

Concretamente, algunas amenazas derivadas del uso de la Inteligencia Artificial por ciberdelicuentes son[102]:

- Utilización de técnicas de *Machine Learning* para diseñar modelos de búsqueda y priorización de objetivos a atacar, analizando las características de acceso y las medidas de protección actuales.
- Las técnicas de neurociencia, porque permiten desarrollar *malware* a medida, optimizando las técnicas de engaño de la ingeniería social para convencer a los usuarios de que accedan a un determinado recurso dónde les espera el *malware* personalizado.
- Utilización de técnicas de *Advanced Intelligent Threat* para el desarrollo de *malware* inteligente.
- Utilización de aplicaciones de Inteligencia Artificial para manipular videos y/o imágenes de personalidades y difundirlos posteriormente a través de las redes sociales creando *fake news*[103] o *deep fakes*[104].

Siete de cada diez empresas[105] están utilizando ya algún tipo de Inteligencia Artificial para la protección de sus activos. La aplicación principal consiste en tareas de detección (de fraude, fugas de seguridad, *malware* avanzado, etc.), reduciendo el tiempo de detección de una brecha de seguridad y ahorrando en los propios costes de detección y respuesta.

---

[101] JUANES, C., DE FUENTES, J.M., SAN JOSÉ, J., "Ciberseguridad: Inteligencia artificial para garantizar la mejor defensa", Marketing y Ventas, núm. 161, mayo de 2020.

[102] Ibidem.

[103] N.B.: *En castellano, bulo.*

[104] N.B.: *Técnica de inteligencia artificial que permite editar vídeos haciendo creer que las personas que aparentemente son reales, utilizando para ello algoritmos de aprendizaje no supervisados a partir de vídeos o imágenes ya existentes.*

[105] CAPGEMINI RESEARCH INSTITUTE, "Reinventing Cybersecurity With Artificial Intelligence", 2019, https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/07/AI-in-Cybersecurity_Report_20190710_V05.pdf

Por su parte, la tecnología *Cloud*[106], como elemento imprescindible del *Big Data* y las soluciones basadas en IA, en tanto solución de almacenamiento, introduce los riesgos propios de la externalización de los servicios (riesgos de seguridad y de privacidad) y los derivados del control de acceso a los datos.

Hasta la aparición de las denominadas tecnologías disruptivas, la protección de los activos de información de una organización quedaba limitada al ámbito del área de informática. Los datos de una compañía solían ser tratados y almacenados en servidores (físicos o virtuales) de la compañía, servidores normalmente ubicados en un Data Center de la empresa, o en un Data Center externo, en modalidad de *hosting*, a lo sumo. Esa área de Tecnologías de la Información controlaba los equipos corporativos (ordenadores de sobremesa o portátiles) desde los cuales se tenía acceso a la información y se podía llegar a tener seguimiento sobre los datos que se transfiriesen, bien a través de correo electrónico (el servidor de correo podía estar en la propia compañía), bien mediante otras redes de comunicaciones (un *Firewall* o cortafuegos podía controlar el único punto de acceso desde el exterior de la compañía, a través de VPN, por ejemplo).

Este escenario ha cambiado completamente en los últimos años. *Cloud Computing* ha permitido deshacerse de los servidores físicos corporativos, trasladando los costes de adquisición y mantenimiento a un coste del servicio, introduciendo, además, el concepto de servicio o aprovisionamiento bajo demanda. El ahorro en costes de almacenamiento ha permitido el uso generalizado del *Big Data*, lo cual ha dado pie al despliegue de capacidades de analítica avanzada en la nube a costes razonables. La movilidad, la interconexión, las redes 4G o el futuro despliegue del 5G o los objetos conectados han difuminado totalmente el perímetro corporativo, multiplicando el número de puntos de acceso a la información. Todo ello, como ya se apuntaba en el apartado anterior, conlleva asociados unos riesgos comunes de seguridad: mayor superficie de exposición, dependencia de las garantías de seguridad de prestadores de servicios externos y diversidad de los sistemas a proteger.

Los sistemas de protección también evolucionan para dar respuesta a las nuevas necesidades tecnológicas. Hemos pasado de los Firewall tradicionales basados en reglas de origen/destino a los Firewall de Nueva Generación (NGFW, por sus siglas en inglés); de los antivirus basados en firmas a los EDR (*Endpoint Detection & Response*); o hemos incorporado soluciones completas para la protección de los servicios SaaS[107] en la nube, conocidas como CASB (*Cloud Access Security Broker*).

Incluso otras tecnologías disruptivas, como *Blockchain*, pueden ayudar a aumentar la seguridad frente a los retos a los que se enfrentan estas mismas tecnologías (como las que nos ocupan: Inteligencia Artificial, Internet de las Cosas, Big Data). En efecto, la Inteligencia Artificial se caracteriza en ayudar o incluso automatizar la toma de decisiones en base a la pretensión de optimizar los procesos mentales que determinarían la decisión más correcta[108], y por otro lado *Blockchain* nos ayuda a verificar, ejecutar y registrar

---

[106] N.B.: *Computación en nube; tal y como la define la RAE, modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de internet a un conjunto de recursos compartidos y configurables de modo escalable (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios, etc.).*

[107] N.B.: *Software como un Servicio (Software as a Service) es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación, a los que se accede vía Internet desde un cliente.*

[108] PWC IDEAS, "Inteligencia artificial y Blockchain, el yin y el yang de la tecnología", 2016, https://ideas.pwc.es/archivos/20161111/inteligencia-artificial-y-blockchain-el-yin-y-el-yang-de-la-tecnologia

las diferentes transacciones digitales que se efectúan. Ambas tecnologías se complementan perfectamente y sin duda su uso puede aportar grandes beneficios a la seguridad de los sistemas: la Inteligencia Artificial proporciona analítica e información a los procesos de toma de decisiones, y *Blockchain* proporciona integridad, seguridad y descentraliza al entorno en el que tienen lugar las transacciones, lo que puede contribuir enormemente a la mejora de los procesos.

2. Riesgos de seguridad específicos.

INTERNET DE LAS COSAS

El Instituto Americano de Estandarización y Tecnologías (NIST, por sus siglas en inglés) publicó en 2019 el documento NISTIR 8228109 sobre la identificación y gestión de los riesgos de privacidad y ciberseguridad en los dispositivos IoT. Establece una clasificación de riesgos atendiendo a los relativos a la seguridad del dispositivo, a la seguridad de los datos y a la privacidad de los individuos. Entre los principales riesgos de seguridad identificados en IoT, podemos citar los siguientes:

- Falta de capacidades de gestión y administración
- Falta de capacidades de monitorización y seguimiento (*logs*)
- Falta de interfaces con el usuario (o no son plenamente funcionales)
- Dificultad para una gestión centralizada
- Amplia variedad de software a gestionar
- Ciclo de vida corto de los dispositivos
- Falta de documentación técnica sobre los dispositivos (dificultad para su reparación)
- Inexistencia de herramientas de inventariado IoT
- Numerosos intervinientes para un mismo servicio (el fabricante del dispositivo, el de la *App*, el prestador de servicios en la nube, el proveedor de telecomunicaciones, etc.)

Por su parte, la Agencia Española de Protección de Datos[110] ha relacionado los principales riesgos para la privacidad y protección de datos en el ámbito de IoT:

- Revelación invasiva de pautas de comportamiento y perfiles
- Falta de control y asimetría de la información
- Participación de múltiples actores con diferentes roles de responsabilidad, lo cual supone dificultad en los niveles de cumplimiento que a su vez puede conllevar más vulnerabilidades en materia de seguridad que puedan suponer una brecha de seguridad de los datos personales.
- Los sistemas IoT pueden afectar no sólo a los usuarios directos de las mismas sino también a aquellos que en algún momento puedan encontrarse "próximos" al sistema o dispositivo.

[109] NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", NISTIR 8228, junio de 2019, https://csrc.nist.gov/publications/detail/nistir/8228/final

[110] AEPD, IoT (I): Qué es IoT y cuáles son sus riesgos, 3 de Diciembre de 2020, https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos

- Falta de medidas de seguridad apropiadas en cualquiera de las capas (dispositivo, comunicación y servicio), bien por las limitaciones de los dispositivos, bien por deficiencias en la aplicación de los principios de protección de datos desde el diseño, como carencia de cifrado en las comunicaciones, contraseñas por defecto, etc. La AEPD señala que esta falta de medidas de seguridad puede conllevar la explotación de vulnerabilidades en el dispositivo permitiendo por ejemplo su manipulación remota o usos ofensivos (DDoS) o ataques directos a la capa de aplicación que impliquen accesos indebidos a datos personales de los usuarios o actuaciones que conlleven una brecha de seguridad.
- Limitaciones o imposibilidad de permanecer en el anonimato, debido a cuestiones tales como la utilización de identificadores únicos y la vinculación de estos entre dispositivos.

La AEPD también ha alertado de los riesgos de IoT en el ámbito de la salud, lo cual ha dado origen al Internet de los Cuerpos (*Internet of Bodies*[111]) definido como el "uso de dispositivos conectados a Internet que monitorizan y/o actúan sobre todas o algunas de nuestras constantes vitales y otros datos biométricos, así como otros indicadores de salud como actividad física, calidad del sueño, actividad deportiva o sedentarismo". Un ataque a este tipo de dispositivos puede causar graves consecuencias en la salud de las personas por lo que, tal y como indica la AEPD, la fiabilidad, robustez y resiliencia de todo el tratamiento en el que se enmarcan los dispositivos debe ser la máxima posible.

INTELIGENCIA ARTIFICIAL

Tal y como se desprende de apartados previos del presente estudio, los riesgos del uso de la Inteligencia Artificial no corresponden únicamente a riesgos de los dispositivos o de las comunicaciones. Desde el punto de vista de la Comisión Europea, los principales riesgos derivados del uso de la inteligencia artificial están relacionados con sus consecuencias en cuanto a la protección de los datos personales, la privacidad, la seguridad de las personas o a la responsabilidad civil[112].

En este sentido, podemos decir que la Inteligencia Artificial se distingue del resto de disciplinas tecnológicas por su capacidad de autoaprendizaje mediante datos de entrenamiento y por la criticidad de las decisiones que puede tomar. Los datos de entrenamiento pueden presentar sesgos, destacando en la parte de seguridad el acceso no autorizado a dichos datos con el objetivo de influir en las predicciones o decisiones que se puedan inferir.

De forma más concreta, la AEPD ha señalado algunas amenazas en materia de seguridad en tratamientos que incorporan Inteligencia Artificial:

[111] AEPD, IoT (II): Del Internet de las Cosas al Internet de los Cuerpos, 11 de Enero de 2021 https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-ii-del-iot-al-iob

[112] COMISIÓN EUROPEA, *Libro Blanco sobre la inteligencia artificial, Op. Cit.*

- Ataques mediante técnicas de envenenamiento de patrones adversos a través del acceso y manipulación de los conjuntos de datos de entrenamiento, de forma previa a la configuración del modelo.
- Troyanos y puertas traseras en el propio código o en las herramientas del desarrollo.
- Accesos al modelo, tanto a nivel de caja negra como de caja blanca para la manipulación de los parámetros del modelo, filtrar el mismo a terceros o ataques a la integridad o disponibilidad de las inferencias
- "*Adversarial machine learning*" referenciado por la AEPD como técnicas de alimentación con datos de ejemplo que para nuestra percepción como humanos puedan ser indistinguibles de datos normales, pero que incluyan pequeñas perturbaciones que fuerzan a la IA a llevar a cabo inferencias erróneas.
- Ataques por imitación de patrones que previamente ya se conoce que serán admitidos por la IA.
- Posibilidad de reidentificación de los datos personales incluidos en el modelo mediante inferencia de pertenencia o inversión del propio modelo.
- Fraude o engaño al sistema de la IA por parte de los interesados en perjuicio de otros.
- Pérdida de confidencialidad de resultados de perfilado o decisiones inferidas por la IA así como logs resultado de las inferencias generadas en la interacción con los interesados[113].

Por otro lado, ENISA, también dispone de un documento específico en materia de riesgos vinculados a IA, que profundiza con una taxonomía de amenazas de alto nivel que incluye 8 categorías, entre otras, Actividad Fraudulenta, Espionaje/Interceptación o también Ataques de tipo físico, Desastres o Interrupciones. Dentro de dichas categorías de alto nivel, se incluyen hasta un total de 74 amenazas, por ejemplo, para el caso de Actividad Fraudulenta, se identifican amenazas relativas al Sabotaje del Modelo o el Envenenamiento del modelo de IA, o, entre otras, para el caso de Interceptación/Espionaje, Revelaciones del Modelo de IA, Inferencia de Datos o Encriptación Débil[114].

Como ejemplos prácticos de algunos de los riesgos de seguridad citados, sería el de evasión de los sistemas antispam a través del cambio de caracteres: por ejemplo, introducir el número "1" en lugar de la letra "i" para obtener "V1agra" (aunque ahora se detecta como spam, en las primeras versiones del ataque sí lo hizo). Un problema potencial mucho más serio sería el que tendrían soluciones con impactos contra la salud del usuario, debido a unas de las características que se ha apuntado anteriormente: los algoritmos de Inteligencia Artificial se usan para la toma de decisiones extremadamente críticas. Por ejemplo, en coches autónomos dependientes de técnicas de visión artificial, se podrían manipular las imágenes recibidas por dichos sistemas (eliminando un signo de STOP en una vía) y provocar así un accidente. Otros ejemplos similares de fraude pueden producirse en procesos de selección, mediante la inclusión de palabras clave sobre méritos falsos en un CV, con una fuente y color invisible a primera vista del humano que visualiza el mismo, pero que sea legible

[113] AEPD, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020, p. 42 a 43. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[114] ENISA, *Artificial Intelligence Cybersecurity Challenges,* diciembre de 2020. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

para el sistema de IA y efectivamente procesado a través de sus filtros previos, descartando a otros candidatos o poniendo al mismo en una situación ventajosa de forma indebida con respecto a los demás[115].

Finalmente, hay que señalar que, como se afirma en el mencionado Libro Blanco de la Comisión Europea, la mayoría de las tecnologías de Inteligencia Artificial, se basan en un "efecto caja negra"[116] y en un comportamiento parcialmente autónomo, aspectos que no ayudan a que se pueda comprobar cómo se ha llevado a cabo una determinada decisión.

Estas características propias de la Inteligencia Artificial dificultan enormemente la eficacia de una revisión para verificar si el proceso de toma de decisiones cumple o no con la normativa de protección de datos. De ahí la importancia de avanzar en técnicas que permitan descubrir la causa raíz de los errores que la Inteligencia Artificial pueda ocasionar tanto por los niveles de la disponibilidad y calidad de los datos, como por los algoritmos de aprendizaje empleados. Las facilidades de revisión son importantes también para probar las relaciones de causa-efecto entre la acción tecnológica y un resultado, especialmente cuando produzca daños a terceros. Esto último se encuadra en la necesidad general de monitorización y gestión de los eventos (logs) sobre los dispositivos, especialmente en sistema convergentes IoT-IA.

En este punto cobran especial importancia las **auditorías algorítmicas** en el sentido de poder prevenir riesgos tanto en materia de seguridad como éticos y legales.

BIG DATA

ENISA cuenta con un documento que analiza las **amenazas** en *Big Data*, se trata de "*Big Data Threat Landscape and Good Practice Guide*"[117], identificando las siguientes:

- Daño no intencionado / Pérdida de información:
  - Fugas de información debido a errores humanos
  - Fugas de datos a través de aplicaciones web (API inseguras)
  - Fallos de diseño o de implementación
- Espionaje / Interceptación de datos:
  - Interceptación de la información
- Actividad fraudulenta:
  - Robo o falsificación de identidad
  - Denegación de servicio
  - Software malicioso (malware)
  - Falsificación de certificados
  - Actividades no autorizadas, abuso de privilegios

---

[115] AEPD, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, 2020, p. 43.* https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[116] N.B.: Es un elemento que se estudia desde el punto de vista de las entradas que recibe y las salidas (interfaz) o respuestas que produce, sin tener en cuenta su funcionamiento interno.

[117] *ENISA – Big Data Threat Landscape and Good Practice Guide (2016):* https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport

  - Fallo en los procesos de negocio
- Legal:
  - Incumplimiento de regulación o legislación
  - Tratamiento no autorizado de datos personales
- Organizacional:
  - Falta de preparación del personal

En relación a los **riesgos** en el uso de la tecnología ***Big Data*** son, además de los mismos que existen en los sistemas tradicionales de tratamiento de datos (véase el documento *Big Data Threats* de ENISA[118]), aquellos consecuencia de sus propios rasgos:

- La escala de datos puede proveer una precisión en la información muy superior a los sistemas tradicionales y es por lo tanto un objetivo muy codiciado por los atacantes para diferentes propósitos (venta en mercado negro, extorsión).
- Esta precisión lleva un paso más allá el detalle de los perfiles de usuarios que construyen los propietarios de las aplicaciones, creando así una asimetría de información entre el usuario y los propietarios de los datos.
- Los datos recogidos en las aplicaciones de *Big Data*, usados para analizar situaciones críticas, pueden ser malinterpretados o usados de forma no adecuada, por ejemplo, a causa de un ataque con el objetivo de generar análisis erróneos que pudieran ser fatales para las empresas que utilizan dichos sistemas.

Parte 5: Gestión de riesgos

Hasta el momento hemos visto los diferentes impactos, éticos, legales y de seguridad, que debemos tener presentes en el uso de tecnologías disruptivas. En el presente apartado, abordaremos la gestión de riesgos teniendo en cuenta los diferentes vectores de impacto comentados.

1. Cumplimiento normativo.

Si algo tienen en común Internet de las Cosas, *Big Data* e Inteligencia artificial es que son tecnologías gracias a las cuales podemos recoger, tratar y analizar ingentes cantidades de información. Como ya afirmó la Comisión Europea[119], a medida que la transformación impulsada por los datos penetra en la economía y la sociedad, cada vez son mayores los volúmenes de datos generados por máquinas o procesos basados en tecnologías emergentes como internet de las cosas, las fábricas del futuro y los sistemas conectados autónomos.

[118] ENISA, *Big Data Security Good Practices and Recommendations on the Security of Big Data Systems*, diciembre de 2015, https://www.enisa.europa.eu/publications/big-data-security

[119] COMISIÓN EUROPEA, "La construcción de una economía de los datos europea", *Op. Cit.*

La Unión Europea es consciente de que los **datos** son un **recurso esencial** para el crecimiento económico, la creación de empleo y el progreso social, hasta el punto de constituir la llamada "Economía de los datos". En palabras de la Comisión Europea[120], "la «economía de los datos» se caracteriza por un ecosistema en el que diferentes tipos de agentes del mercado –como fabricantes, investigadores y proveedores de infraestructuras– colaboran para garantizar que los datos sean accesibles y utilizables. Esto permite a dichos agentes extraer valor de esos datos, creando toda una gama de aplicaciones con un gran potencial para mejorar la vida cotidiana".

Es por ello que Europa ha sido consciente de la necesidad de un marco jurídico claro que permitiese la libre circulación de datos y el acceso a grandes conjuntos de datos dentro de la UE removiendo así los posibles obstáculos a la innovación y creación de empresas, y por tanto a la Economía de los datos.

DATOS PERSONALES

Tal y como se ha mencionado en el apartado relativo a los impactos legales, y concretamente, en materia de protección de datos y privacidad, debemos tener muy presente el **Reglamento 679/2016 General de Protección de Datos** (RGPD), complementado en el caso nacional, por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). y la todavía propuesta de Reglamento ePrivacy[121] como ejes que marcan las bases de los requerimientos normativos en este ámbito.

Aspectos como el deber de información, de obtención del consentimiento, la transparencia y limitación de la finalidad en el tratamiento de los datos de carácter personal son cruciales.

En una visión de tipo práctica, se debe analizar especialmente cómo cumplir con el **deber de información** sobre el tratamiento de datos conforme al **principio de transparencia** o en su caso, el **consentimiento**, pues supone todo un reto dadas las características físicas del dispositivo. Pensemos, por ejemplo, en un reloj de pulsera conectado con una pantalla pequeña o en un dispositivo sin interfaz visual.

Finalmente, en lo que respecta a la limitación de la finalidad, resulta esencial especialmente en cadenas cada vez más complejas de actores y soluciones tecnológicas que puedan integrar un sistema de IoT, Big Data e IA, que existan mecanismos y garantías suficientes para asegurar que las ingentes cantidades de datos aportadas por los usuarios, no se destinen a finalidades distintas incompatibles con las inicialmente informadas al usuario final.

DATOS NO PERSONALES

La cuestión de la libre circulación de datos como presupuesto para el desarrollo de la Economía de los datos, afecta a todos los tipos de datos, no sólo a los personales, por lo que el marco jurídico ha sido completado con

[120] Ibídem

[121] COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas..., *Op. Cit.*

el Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

Su objeto[122] de aplicación son aquellos tratamientos de datos electrónicos que no tengan carácter personal, que se presten como un servicio a usuarios que residan o tengan un establecimiento en la UE, o se efectúe por una persona física o jurídica que resida o tenga un establecimiento en la Unión para sus propias necesidades. Este Reglamento no se aplicará a servicios de tratamiento de datos que tenga lugar fuera de la UE.

Como puede observarse, al hablar de "datos **electrónicos que no tengan carácter personal**" se hace una definición en negativo, por lo que el *Reglamento 679/2016 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* (en adelante, RGPD) se aplicará en el momento en que podamos estar ante datos de carácter personal, según la definición dada por el RGPD. Esto no quiere decir que, en caso de estar ante datos de carácter personal, el Reglamento 2018/1807 deje de ser de aplicación, pues como aclara[9] el propio texto legal, en caso de estar ante un conjunto de datos personales y no personales (sobreentendemos conjunto diferenciado), el Reglamento 2018/1807 se aplicará a los datos no personales y en el caso de que los datos de dicho conjunto estén "inextricablemente ligados", ambos Reglamentos serán de aplicación[123].

PROPIEDAD INTELECTUAL

Los necesarios principios de transparencia en la toma de decisiones por parte de sistemas de IA, ya en parte anticipados por el RGPD en su artículo 13, como un requisito de información necesario para el interesado: *"(...) f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.(...)"*, plantean un reto sobre la protección del trabajo y la autoría de los sistemas de IA, que en ocasiones son los pilares de distintos modelos de negocio y que sin la adecuada protección jurídica frente a prácticas de espionaje encubiertas fraudulentamente en ejercicios de derechos, pueden dar lugar a importantes desequilibrios competitivos en la industria 4.0.

Si bien los programas de ordenador pueden ser objeto de protección mediante propiedad intelectual, su creación debe ser original[124], planteando retos adicionales para el caso de un algoritmo que es capaz de "automejorarse" mediante la retroalimentación de otros códigos informáticos que puedan ser de creación de terceros. En el mismo sentido de esta capacidad de creación "autónoma" que pueda desarrollar el sistema de

[122] N.B.: *Vid.* artículo 2.1 del Reglamento 2018/1807.

[123] LOZA CORERA, M., "Hacia la economía de los datos europea...", *Op. Cit.*

[124] N.B.: La Ley de Propiedad Intelectual (LPI), en su artículo 96.2 establece: "El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor".

IA, se plantean otros retos como la autoría de una obra artística creada por un algoritmo, puesto que el sistema de IA no ostenta capacidad jurídica para ser titular de derechos y obligaciones[125,126].

SECRETOS EMPRESARIALES

La ingente capacidad para el procesamiento de información de los sistemas de big data, puede generar contenido agregado de alto valor añadido, por ejemplo, en forma de *know-how* e información de valor estratégico, económico y competitivo para la entidad explotadora del mismo. Para el caso de que no fuera de aplicación la normativa de protección de datos, podría ser de aplicación la protección de la legislación sobre secretos empresariales[127]. La información que podamos obtener como resultado de análisis de *big data* o IA, puede inferir adicionalmente en información concreta y de alto valor, por ejemplo: estimaciones de mercado, riesgos, etc. que pueda ser susceptible de protección por la normativa de secreto empresarial, en el sentido de que no sea información normalmente conocida ni accesible, al necesitar grandes capacidades de procesamiento, y en consecuencia tenga un especial valor empresarial, por ejemplo: si nos da indicadores sobre cómo y cuándo llevar a cabo determinadas inversiones económicas y, finalmente, condicionado por las anteriores circunstancias, se establezcan medidas razonables para mantener su secreto, donde como hemos dicho, será crítica la buena implementación de un Sistema de Gestión de la Seguridad de la Información, ya no solo para la protección de datos de carácter personal, sino para la protección de información que no necesariamente es de carácter personal, pero tiene un alto valor para la organización.

RESPONSABILIDAD CIVIL

Una de las cuestiones que destaca la Comisión Europea, tanto en su documento *Libro Blanco sobre la inteligencia artificial*[128] y de forma más concreta, en su documento *Liability for Artificial Intelligence and other emerging digital technologies*[129], son los nuevos retos en materia de responsabilidad civil que se plantean por el uso de la IA[130].

---

[125] GUADAMUZ, A., "La inteligencia artificial y el derecho de autor", OMPI revista, octubre de 2017, https://www.wipo.int/wipo_magazine/es/2017/05/article_0003.html

[126] N.B.: *Según la LPI, artículo 5:* "1. Se considera autor a la persona natural que crea alguna obra literaria, artística o científica.2. No obstante, de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella".

[127] N.B.: *La Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que traspone la Directiva (UE) 2016/943, de 8 de junio, define los secretos empresariales como:* "(...) cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.(...)".

[128] COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial, *Op. Cit.*

[129] COMISIÓN EUROPEA, *Liability for Artificial Intelligence and other emerging digital technologies,* Expert Group on Liability and New Technologies, 2019, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

[130] N.B.: En este sentido se cita la Directiva del Consejo de 25 de julio de 1985 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, traspuesta en nuestro ordenamiento jurídico a través de la Ley 22/1994, de 6 de julio, que fue derogada por el actualmente vigente Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Se citan también la Directiva 2014/104/UE del Parlamento Europeo y del Consejo de 26 de noviembre de 2014 relativa a determinadas normas por las que se rigen las acciones por daños en virtud del Derecho nacional, por infracciones del Derecho de la competencia

Un punto especialmente controvertido y que a su vez resulta muy ilustrativo sobre la aplicación práctica de la IA y la legislación, son los denominados **coches autónomos**, especialmente en supuestos de responsabilidad civil derivada de los accidentes. Ni el marco legislativo europeo ni nuestra legislación nacional (*Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor*), dan respuesta expresa, como es lógico por razón de su contexto histórico. Quizá una de las mayores aproximaciones de nuestras instituciones nacionales al contexto práctico de los vehículos autónomos haya sido por parte de la Dirección General de Tráfico (DGT), a través de las instrucciones *INSTRUCCIÓN 15/V-113* sobre *Autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general*[131] e *INSTRUCCIÓN 16 TV/89 sobre Estacionamiento asistido de vehículos a motor*[132].

TRANSPARENCIA

En el sector público, el debate sobre la transparencia de las decisiones de la IA puede adquirir una mayor entidad en el contexto del sector público y el uso de dicha tecnología, especialmente si tenemos en cuenta la legislación en materia de transparencia a nivel estatal y autonómica.

Si atendemos a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno "Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones". En vista del artículo expuesto, si un Ayuntamiento hubiera desarrollado un sistema de IA para multar por el incumplimiento de determinadas ordenanzas, ¿podríamos exigir como ciudadanos conocer los fundamentos de los algoritmos del sistema de IA en base a la Ley de transparencia? O bien ¿Podríamos plantear límites para evitar que precisamente un estudio demasiado profundo del sistema pudiera facilitar a los ciudadanos aprovechar defectos del mismo y vulnerar las ordenanzas que se supone que la IA debería hacer cumplir?

AUDITORIA Y SEGURIDAD

Las herramientas de gobierno del dato son un elemento facilitador de auditorías y posibles análisis de impacto. En estas herramientas se gestiona el nivel y tipo de acceso de los usuarios a recursos de datos, así como el uso que cada grupo de usuarios hace de los mismos. Desde algunas de ellas pueden generar informes que reflejen la seguridad implementada a nivel de cada elemento tecnológico y la seguridad aplicada a cada rol y grupo de usuarios, siendo el punto de entrada ideal para hacer una auditoría corporativa general sin tener que recorrer toda la infraestructura.

---

de los Estados miembros y de la Unión Europea, traspuesta en nuestro ordenamiento jurídico a través del Real Decreto-ley 9/2017, de 26 de mayo, con afectación en distintos cuerpos legislativos.

[131] DGT, "Instrucción 15/V-113 sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general", *Op. Cit.*

[132] DGT, "Instrucción 16 TV/89 sobre estacionamiento asistido de vehículos a motor", Dirección General de Tráfico del Ministerio del Interior, 20 de enero de 2016, http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/2016/Instruccion_16_TV_89_Estacionamiento_asistido_vehiculos_motor.pdf

También destacan por su importancia en esta materia las **auditorías de algoritmos** a través de las que podamos evidenciar el cumplimiento de los requerimientos normativos tanto en materia de protección de datos como de la **propuesta de Reglamento de Inteligencia Artificial** y otras normas, pero también de aspectos técnicos y éticos, en línea con lo establecido por el Grupo de Expertos de Alto Nivel de Inteligencia Artificial[133] y los siete requisitos para lograr una IA fiable y por supuesto con la propuesta de Reglamento de Inteligencia Artificial.

2. Normalización: ISO y Certificaciones.

El actual avance *in crescendo* e imparable de los usos actuales y futuros de las tecnologías disruptivas está generando importantes retos y desafíos en diferentes campos, como pueden ser el social, el económico y el regulatorio.

Aspectos relacionados con su confiabilidad, seguridad y privacidad, junto con la toma de decisiones basadas en complejos procesos de análisis de datos o las temidas repercusiones en el mundo laboral, hacen que tanto los diferentes organismos regulatorios afectados como los gobiernos, estén trabajando conjuntamente y sean conscientes de dar un enfoque coordinado e internacional al mismo.

En palabras de José Antonio Jiménez – Técnico de Normalización de Electrónica y TIC: "La normalización ayuda a la implantación masiva de los avances tecnológicos en la sociedad. En estos momentos, se está produciendo una revolución en la incorporación de la tecnología de la información a todos los sectores productivos, tanto tradicionales como de nueva creación. De entre la multitud de tecnologías, hay dos que tienen una especial relevancia: la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT). La introducción de estas tecnologías en el mundo real se enfrenta a retos como la interoperabilidad, la seguridad, los riesgos asociados o las implicaciones éticas y sociales. Para todos estos desafíos, los estándares aportan las soluciones que se necesitan"[134].

Referencias en este sentido son las líneas de trabajo y competencias de los subcomités SC41 y SC42 pertenecientes al comité ISO/IEC JTC 1135, comité consagrado de referencia internacional cuyo propósito es desarrollar, mantener y promover estándares en el campo de las Tecnologías de la Información (TI) y las Tecnologías de la Información y las Comunicaciones (TIC) y que está constituido de forma conjunta por la Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

- ISO / IEC / JTC 1 / SC 41: Internet de las cosas y tecnologías relacionadas.
- ISO / IEC / JTC 1 / SC 42: Inteligencia Artificial.

El subcomité SC 41 se creó en 2016 fruto de la unión de dos grupos de trabajo del JTC 1, el de redes de sensores (WG 7) y el de IoT (WG 10). Su función es la de apoyar a los comités de estandarización en materia de IoT y tecnologías relacionadas, incluyendo las redes de sensores y los wearables. En la actualidad cuenta con 18

[133] High-Level Expert Group on AI, *Ethics guidelines for trustworthy AI*, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[134] JIMÉNEZ, Jose Antonio, "Impulso español a las normas mundiales sobre IA, Big Data e IoT", UNE *La revista de la normalización española*, enero de 2020, https://revista.une.org/21/impulso-espanol-a-las-normas-mundiales-sobre-ia-big-data-e-i.html

[135] ISO, "ISO/IEC JTC 1Information Technology", International Organization for Standardization. https://www.iso.org/isoiec-jtc-1.html

programas de trabajo activos[136] que van desde la propuesta de la arquitectura de referencia IoT hasta requerimientos de compatibilidad entre dispositivos pasando, por ejemplo, por la integración entre IoT y Blockchain.

El subcomité SC 42 se creó en el año 2017 con el objeto de elaborar normas internacionales que sirvan de referencia en el ámbito del desarrollo del ecosistema de Inteligencia Artificial. Los temas que forman parte del trabajo de este subcomité son: Estándares fundamentales, enfoques computacionales y características de IS; casos de uso y aplicaciones; Big Data y Preocupaciones sociales[137].

La convergencia de distintas tecnologías es una de las cuestiones que abordan los subcomités. Ya se ha citado el grupo de trabajo sobre IoT y Blockchain, del subcomité SC 41 de ISO/IEC JTC 1 o el documento (en desarrollo) "Tecnología de la información – Inteligencia artificial Marco de gestión de procesos para análisis de Big Data" del subcomité SC 42 de ISO /IEC JTC 1.

Ya en 2015[138] ENISA señalaba la falta de estandarización como uno de los retos en los modelos de infraestructura y almacenamiento de *Big Data*. A lo que añade la preocupación por la portabilidad de los controles de seguridad entre diferentes proveedores o, incluso, en proyectos *Open Source* (como Hadoop[139], por ejemplo).

En este sentido, ENISA ya apelaba a la estandarización en el documento "Big Data Security"[140] de diciembre de 2015. Entre las recomendaciones de seguridad, la siguiente: "Recomendación 4: Las entidades de estandarización deberían adaptar los estándares de seguridad existentes, o crear estándares nuevos, para Big Data. Actualmente no hay certificaciones específicas para Big Data, así que los estándares ayudarán a la industria del sector a avanzar y proveer mejores servicios a los usuarios". Si bien ENISA reconoce la inexistencia de certificaciones en Big Data, la misma agencia propone tomar como punto de partida el listado de certificaciones en Cloud Computing, que está disponible a día de hoy[141].

La interoperabilidad es otra de las preocupaciones de los reguladores. El Instituto Nacional de Estándares y Tecnología norteamericano (NIST, por sus siglas en inglés) ha publicado su propio marco de interoperabilidad: "*The NIST Big Data Interoperability Framework (NBDIF)"* con el propósito de crear herramientas que puedan analizar datos con independencia de la plataforma en la que se encuentren y que tanto los datos (*Big Data*) como la analítica (Inteligencia Artificial) puedan moverse de plataforma de una forma fácil y ágil.

---

[136] IEC, "ISO/IEC JTC 1/SC 41 Work programme", https://www.iec.ch/dyn/www/f?p=103:23:8187723854992::::FSP_ORG_ID,FSP_LANG_ID:20486,25

[137] IEC. *Artificial intelligence across industries*. International Electrotechnical Comission Whitepaper. https://basecamp.iec.ch/download/iec-white-paper-artificial-intelligence-across-industries-en/

[138] ENISA, *Big Data Threat Landscape and Good Practice Guide*, enero de 2016, https://www.enisa.europa.eu/publications/bigdata-threat-landscape

[139] N.B.: vid https://hadoop.apache.org

[140] ENISA, *Big Data Security, op. cit.*

[141] ENISA, "Cloud Computing Certification - CCSL and CCSM", https://resilience.enisa.europa.eu/cloud-computing-certification

La Comisión Europea también ha tratado la cuestión de la interoperabilidad en la comunicación "Una Estrategia Europea de Datos"[142]. La interoperabilidad y la calidad de los datos, así como su estructura, autenticidad e integridad son clave para la explotación del valor de los datos, especialmente en el contexto del despliegue de la Inteligencia Artificial.

Para las tecnologías IoT, la ISO cuenta ya con estándares específicos para estas tecnologías:

- ISO 30141:2018: Arquitectura de Referencia IoT
- ISO 20924:2018: Vocabulario IoT
- ISO 21823-1:2019: Interoperabilidad de IoT (Parte 1: Framework)
- ISO 22417:2017: Casos de uso de IoT

Aunque en algunos de estos estándares se encuentran ciertas referencias a la seguridad y a la privacidad (como en el capítulo 6.5.3 de ISA 28123: "Protección de datos personales"; o el capítulo 11.4 de ISO 30141: "Datos personales y privacidad de la información") el subcomité ISO/IEC JTC 1/SC 27 está desarrollando la futura norma ISO 27030 "Directrices de seguridad y privacidad en IoT" (actualmente en fase de evaluación del *Working Draft* por parte del Comité) que establecerá un conjunto de objetivos, directrices y controles para asegurar la privacidad y la seguridad de los entornos IoT.

El NIST cuenta también con un documento de referencia: NISTIR 8228: Consideraciones para la gestión de los riesgos de ciberseguridad y privacidad de Internet de las cosas (IoT)[143].

Con el fin de resolver o al menos mitigar los problemas de interoperabilidad e integración comentadas, se puede aplicar un marco de gobierno del dato, como por ejemplo el ofrecido por DAMA[144]. DAMA ofrece recomendaciones y aplicación de buenas prácticas para once disciplinas, siendo una de ellas precisamente la interoperabilidad e integración de datos.

[142] COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", *Op. Cit.*

[143] NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", *Op. Cit.*

[144] https://www.dama.org

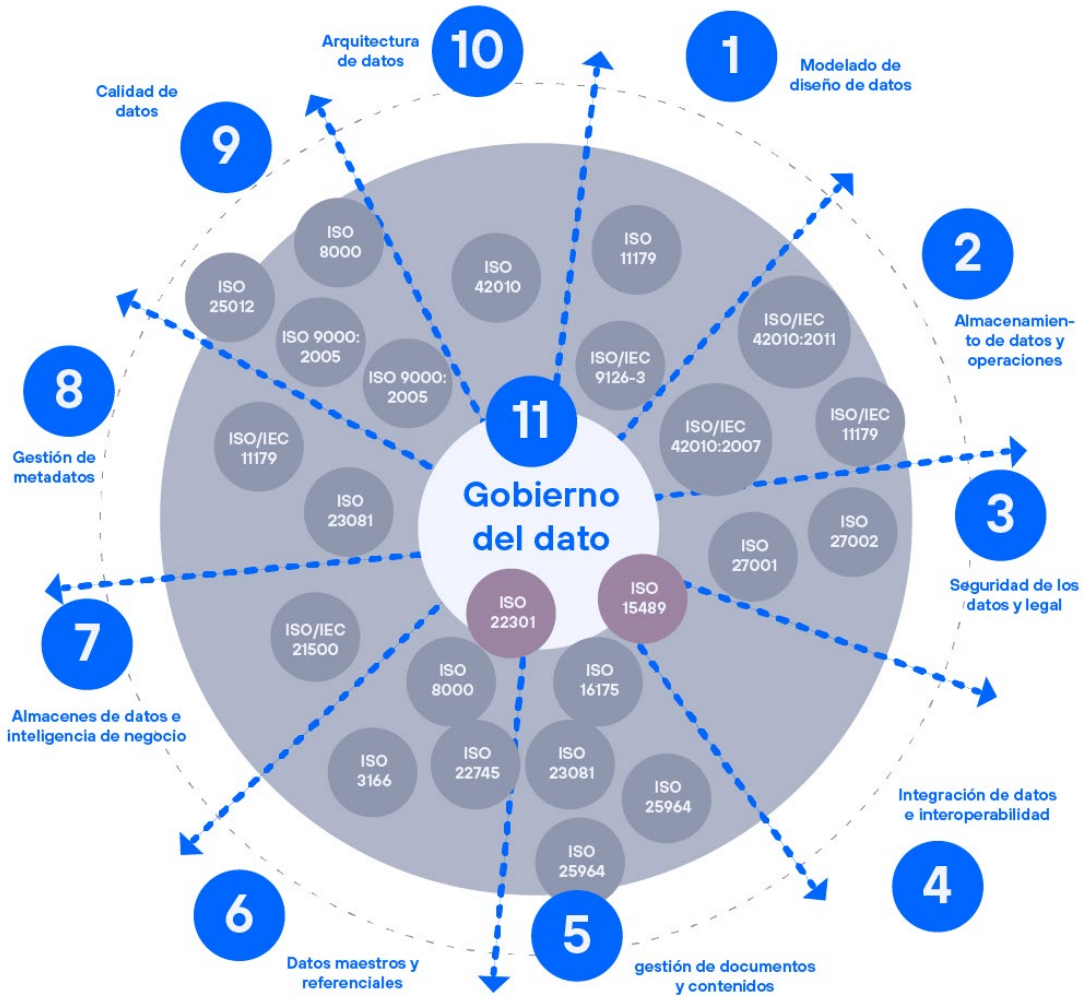

Figura 5: ISOS que aplican a las disciplinas DAMA de Gobierno del Dato. Fuente: DGU - Telefónica Tech IA of Things

3. Autorregulación mediante nuevas certificaciones.

Carlos Manuel Fernández (Asesor Estratégico de TI en AENOR) y Boris Delgado Riss (Gerente de TIC en AENOR) son de la opinión de que "El avance y evolución de las Tecnologías de la Información y Comunicación no cesa y su vertiginoso desarrollo es de tal magnitud, que la cuarta revolución industrial y la Transformación Digital están teniendo un profundo impacto en las organizaciones, en las industrias y en la sociedad". Hacen referencia a los nuevos escenarios tecnológicos como SMAC (*Social-Mobility-Analytics-Cloud*), al desarrollo de la denominada Industria 4.0 (OT-Tecnologías de la Operación + IoT-Internet de las Cosas), a las mejoras en los sistemas de comunicación como 5G y al avance de los modelos de Inteligencia Artificial y Machine Learning. Todo ello, dirigido por los datos (*Data-Driven*), configura un escenario donde surgen nuevas

ciberamenazas y ciberriesgos en esta R-Evolución Digital; y es que se trata de una revolución considerando la evolución continua digital[145].

En este sentido AENOR ha diseñado un Ecosistema de Ciberseguridad y Privacidad, basado en estándares/normas internacionales ISO, así como en actuales leyes y reglamentaciones españolas y europeas[146].

Desde ENISA[147] se refiere a la necesidad de inversión de las partes interesadas en incrementar las competencias en seguridad de los profesionales de Big Data, a través de formación y certificaciones. El crecimiento previsto de Big Data en los próximos años requerirá más profesionales cualificados, lo que irá ligado a mayores inversiones en formación y certificación para garantizar entornos de Big Data seguros.

Los CISO, además de definir las apropiadas medidas de seguridad, deberán alinear sus sistemas con el cumplimiento de los adecuados estándares de seguridad. Será crucial tener una visión conjunta de la interrelación de todas las tecnologías implicadas: IoT, Inteligencia Artificial, Big Data, etc.

Desde la Comisión Europea, tanto para IoT como para Inteligencia Artificial se propone un sistema de evaluación de riesgos y de control previo o posterior voluntario. Gracias a la normalización se pueden definir mejor los niveles de riesgo que implica la tecnología IoT tanto para seguridad como para privacidad. Las auditorías pueden dar respuesta al cumplimiento en sistemas complejos que aglutinan varias tecnologías.

4. Autorregulación mediante la ética.

INICIATIVAS

Para hacer frente a las situaciones comentadas en el apartado relativo al Impacto Ético, diferentes organismos y empresas han lanzado iniciativas para asegurar un uso ético de la Inteligencia Artificial que ponga a las personas como prioridad. En la página web Algorithmwatch.org148 (organismo sin ánimo de lucro cuyo objetivo es evaluar el impacto social de la IA) se puede encontrar un inventario de tales iniciativas que incluyen administraciones públicas, organismos internacionales o fabricantes que quieren demostrar su preocupación.

Una de las iniciativas más importantes es la Guía Ética para una Inteligencia Artificial de Confianza definida por el Alto Grupos de Expertos en IA (de sus siglas en inglés HLEG149). Esta guía proporciona a los desarrolladores y usuarios de la Inteligencia Artificial una guía útil a través de una serie de principios y

[145] DELGADO RISS, Boris y FERNÁNDEZ, Carlos Manuel, "ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad", *AENOR, La revista de la evaluación de conformidad*, mayo de 2019, núm 348. Online: https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html

[146] N.B.: vid https://www.aenorciberseguridad.com/certificacion1.html

[147] ENISA, *Big Data Security..., Op. Cit.*

[148] N.B.: Vid. https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/

[149] COMISIÓN EUROPEA, "High-Level Expert Group on Artificial Intelligence", https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

requisitos150. Los cuatro principios de la guía son el respeto de la autonomía humana, la prevención de daño, la equidad y la explicabilidad. Por su parte, los seis requisitos son la acción y supervisión humanas, la solidez técnica y seguridad, la gestión de la privacidad y datos, la transparencia, la diversidad/no discriminación, el bienestar social y la rendición de cuentas[151].

La imagen que se muestra a continuación resume el marco de diseño para una IA fiable de dicha guía en la que se tiene muy presente el impacto ético de las soluciones de IA:

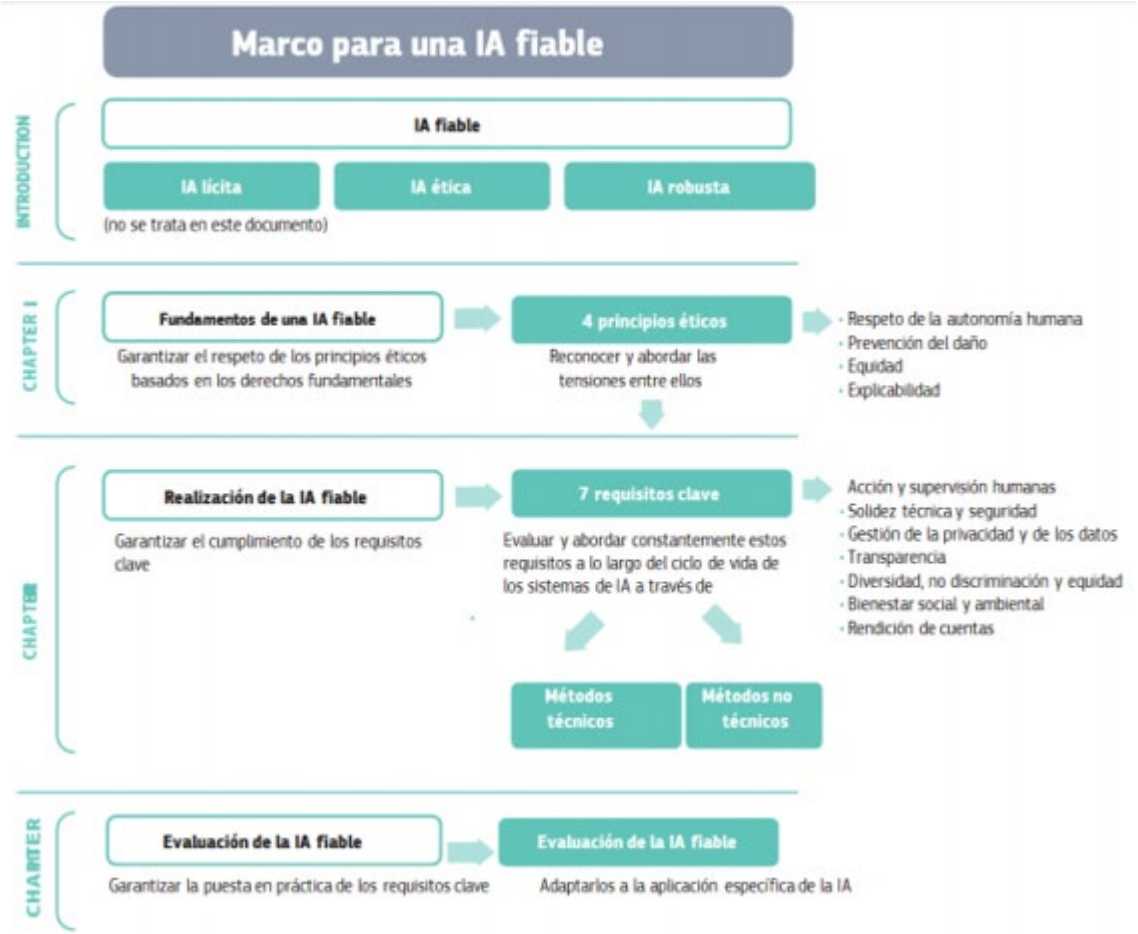

Figura 6: Marco para una IA fiable. Fuente: COMISIÓN EUROPEA, *Directrices éticas para una IA fiable*, pág. 10.

[150] COMISIÓN EUROPEA, *Directrices éticas para una IA fiable..., Op. Cit.*

[151] GOÑI SEIN, J.L., *Defendiendo los derechos fundamentales frente a la Inteligencia Artificial*, Universidad de Navarra, lección de 13 de septiembre de 2019, https://www.unavarra.es/digitalAssets/244/244921_100000Leccion-inaugural-Castellano-19-20_web.pdf

En España, la estrategia de Inteligencia Artificial para I+D+i[152] también recoge, entre sus 6 prioridades, el análisis ético de las aplicaciones de IA de manera que eviten varias de las situaciones problemáticas vistas y recogidas por la Guía de la UE: evitar sesgos negativos y prejuicios de género u otras formas de discriminación, estar alineadas con aspectos éticos o redactar un código ético de la IA en los próximos años.

En septiembre de 2019 también surgió en España la iniciativa OdiseIA[153], con el objetivo de crear una red de colaboración de empresas, organismos y personas que fueran un observatorio del impacto social y ético de la IA en nuestro país.

Empresas privadas como Telefónica también han definido la ética en la IA dentro de sus compromisos de responsabilidad social[154]. Los principios para el desarrollo de soluciones y servicios de IA están alineados con los principios de negocio, y abarcan la transparencia, la explicabilidad, los derechos humanos, la privacidad o la seguridad.

De la misma manera, las grandes empresas tecnológicas como Google[155], IBM[156], Facebook[157], o Microsoft[158] han lanzado de forma pública su compromiso para seguir principios de desarrollo éticos y responsables.

DESAFÍOS

Si bien el problema está claramente definido (la Inteligencia artificial, más allá de los beneficios que puede aportar, tiene impactos éticos que son muy críticos en la vida de las personas) y las empresas y gobiernos están lanzando múltiples iniciativas que muestran su compromiso para hacerle frente, queda todavía camino para alcanzar una forma de control similar a la que existe en el ámbito de la seguridad y privacidad.

Por un lado, no existen regulaciones al respecto y por otro, no se ha determinado la manera en la que se puede auditar el cumplimiento por parte de terceros de confianza. En estos momentos su aplicación depende principalmente de la buena voluntad de las empresas y del nivel de concienciación que puedan tener los usuarios con el objetivo de constituir un medio de debate y presión. Junto a ello, las **auditorías éticas de algoritmos** resultan una pieza imprescindible para contribuir a la confiabilidad de las soluciones de IA.

[152] GOBIERNO DE ESPAÑA, *Estrategia Española de I+D+i en Inteligencia Artificial*, Ministerio de Ciencia, Innovación y Universidades, 2019, https://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pdf

[153] N.B.: *vid. online* https://www.odiseia.org

[154] N.B.: *vid.* https://www.telefonica.com/es/web/negocio-responsable/nuestros-compromisos/principios-ia

[155] N.B.: *vid. online* https://ai.google/principles/

[156] N.B.: *vid. online* https://www.ibm.com/thought-leadership/institute-business-value/report/ai-ethics

[157] N.B.: *vid. online* https://ai.facebook.com/

[158] N.B.: vid. online https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6

5. Concienciación social

Los datos son el nuevo petróleo, como se afirma de forma metafórica para evidenciar el creciente valor que se les atribuye y que cuya explotación dominan no solo las cinco grandes compañías tecnológicas occidentales –Google, Amazon, Facebook, Apple y Microsoft (conocidas por el acrónimo GAFAM)–, sino que es algo que ya ha llevado a algunos a hablar de "la nueva guerra fría" cuando se refieren a la competencia entre China y Estados Unidos por el desarrollo de la IA, a raíz de *Big Data* e IoT.

La irrupción de la capacidad para la explotación de los datos masivos es el hito que marca un nuevo antes y después de nuestro desarrollo civilizacional. Ocurre en paralelo a la máxima elevación como categoría jurídica de un valor cultural de las sociedades occidentales, la privacidad, que no se encuentra en regímenes como el de China o Rusia[159]. Este presupuesto, configurado en nuestro país como derecho fundamental[160], ha sido objeto de un amplio debate teórico y –en la práctica– condiciona, limita, socaba o hasta impide la plena realización de proyectos de *Big Data*.

Uno de los primeros encontronazos gira en torno al concepto de **confianza**[161]. Lo que consideramos fiable o no –seguro o inseguro– varía según nuestro punto de vista. Por ejemplo, el conflicto de derechos cobra una nueva perspectiva desde el momento que la explotación masiva de los datos contribuye a salvar vidas: gracias a *Big Data*, el dato de salud puede decirse que es ya –en términos metafóricos– un verdadero patrimonio de la humanidad[162]. Lo mismo podría decirse de las aplicaciones de Inteligencia Artificial que, en la ponderación entre el derecho a la salud y el de protección de datos, ponderan a favor de todo aquello que está ayudando a combatir la pandemia del coronavirus.

Por otra parte, desde el punto de vista de los sistemas regulatorios, el cambio que generan las tecnologías disruptivas supone toda una serie de efectos[163]: aportan soluciones a problemas regulatorios al hacer innecesarios algunos de los requisitos regulatorios anteriores; revelan vacíos legales existentes; desafían las modalidades de control regulatorio; cuestionan las atribuciones tradicionales de las autoridades reguladoras; ponen en duda la eficacia de las técnicas regulatorias... Cuando menos, al tiempo que ofrecen grandes expectativas de beneficio social y económico, encierran la gran incertidumbre de los costes potenciales.

Dos encuestas realizadas recientemente: la primera la del Eurobarómetro, realizada en marzo de 2019 – justo un año después de la entrada en vigor del Reglamento Europeo de Protección de Datos– y la segunda la del Centro de Investigaciones Sociológicas español[164], realizada en mayo de 2018 sobre cuestiones variadas, dedican un amplio apartado a la percepción sobre la protección de datos de carácter personal.

---

[159] CRAIG, T., LUDLOFF, M. E., Privacy and Big Data, O'Reilly, Sebastopol (CA), 2011, págs. 19-20.

[160] N.B.: Artículo 18.4 de la Constitución Española de 1978, en relación con las Sentencias del Tribunal Constitucional números 290 y 292, de 30 de noviembre de 2000.

[161] SCHNEIER, B., "Technologists vs. Policy Makers", IEEE Security & Privacy, vol. 18, January-February 2020, págs. 71-72.

[162] DE MONTALVO JÄÄSKELÄINEN, F., *Op. Cit.*

[163] MASHAW, J. L., "Prólogo", en: Recuerda Girela, M. A., Tecnologías disruptivas: Regulando el futuro, Aranzadi, Pamplona, págs. 41-43.

[164] CIS, Barómetro de mayo de 2018, estudio nº 3213, http://datos.cis.es/pdf/Es3213mar_A.pdf .

En términos generales, el tema que más preocupa a los españoles es la protección de datos personales y el posible uso de información personal por otras personas, con una clara diferencia respecto a los otros dos temas que le siguen: avances de la ciencia y la tecnología o el desarrollo de la comunicación e información a través de Internet.

Sin embargo, respecto al conocimiento sobre la normativa que protege esta esfera esencial de las personas, a nivel europeo los resultados[165] indican que los encuestados conocen relativamente bien las nuevas normas de protección de datos, sus derechos y la existencia de autoridades nacionales de protección de datos, a las que pueden dirigirse para buscar ayuda en caso de vulneración de sus derechos. Ello se plasma en que el 67 % conoce la existencia del RGPD, aunque de éstos solo el 36% sabe qué es el Reglamento mientras que el 31% ha oído hablar de él pero no sabe qué es exactamente.

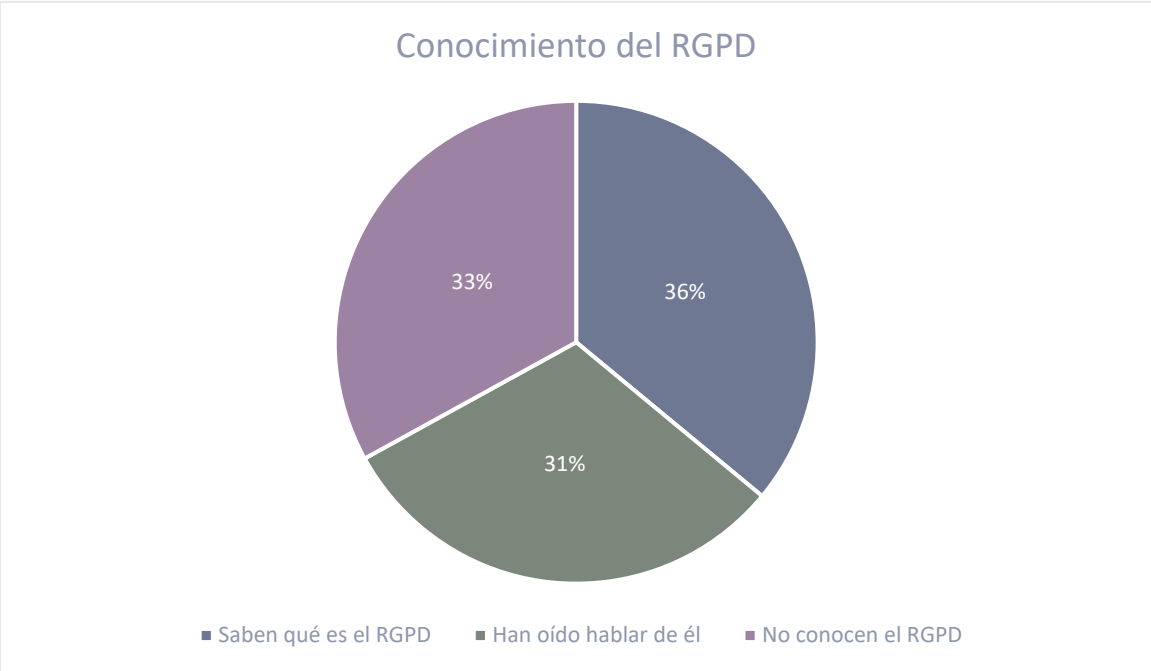

Figura 7: Elaboración propia.

En este contexto, cerca de seis de cada diez europeos (57 %) dicen haber oído algo sobre la existencia de una autoridad pública en su país responsable de proteger sus derechos relativos a sus datos personales. Aun así, según los datos del CIS (2018) solo el 4% de los españoles acudiría en primer lugar a esta autoridad en el caso

[165] Todos los resultados que se citan del Eurobarómetro han sido consultado y extraídos de: COMISIÓN EUROPEA, "487a. General Data Protection Regulation - 487b. Charter of Fundamental Rights", *Public Opinion*, marzo de 2019, https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222

de sufrir algún tipo de problema con sus datos personales, mientras que el 51% recurriría primero a la Policía o la Guardia Civil.

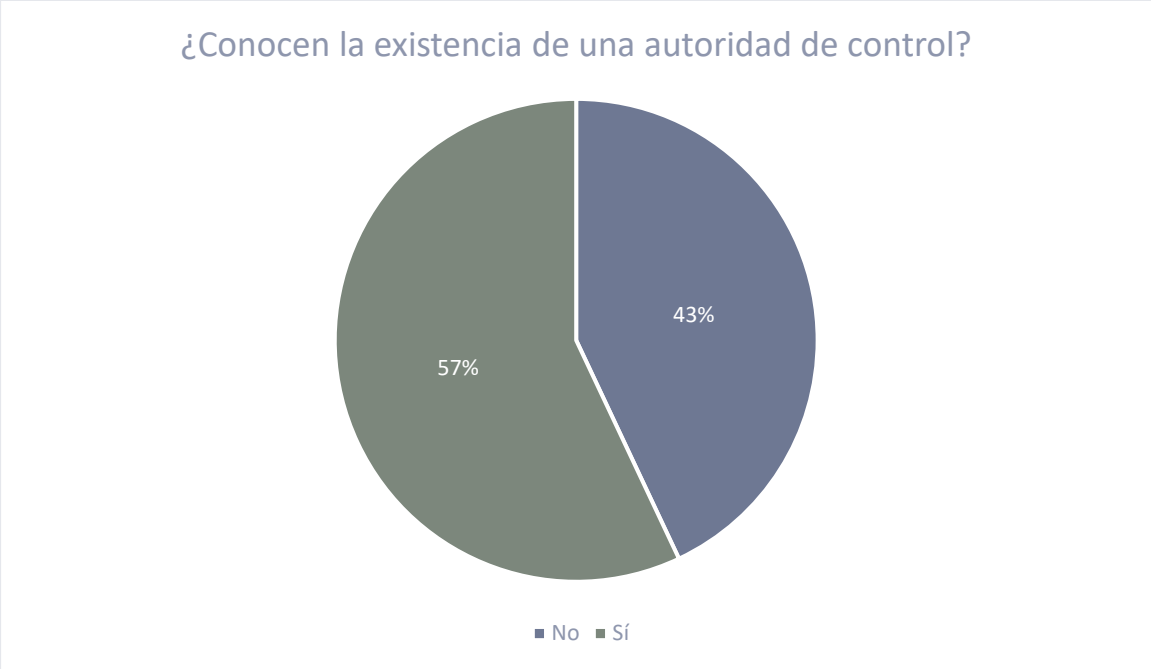

Figura 8: Elaboración propia.

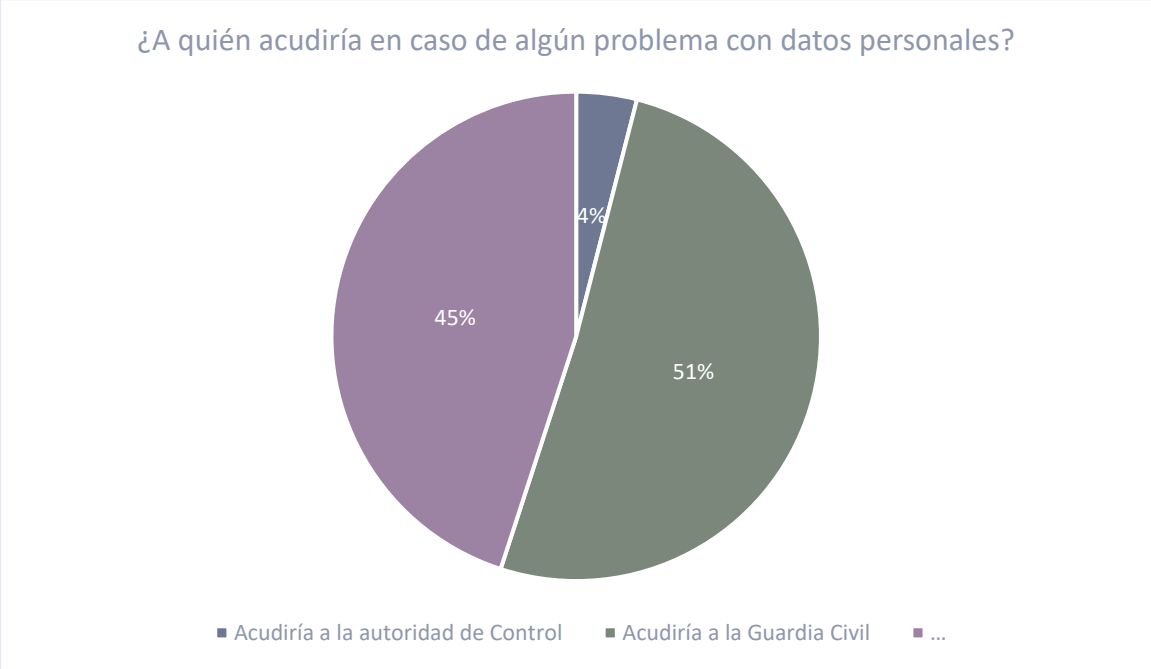

Figura 9: Elaboración propia

En el caso español, respecto a las políticas de privacidad que se muestran al solicitar datos personales en Internet, únicamente el 9 % de los usuarios de Internet reconoce leerlas completamente, mientras que un 40 % afirma leerlas parcialmente, lo cual implica que la mitad de los internautas españoles no lee nada de estos apartados y declaraciones de privacidad.

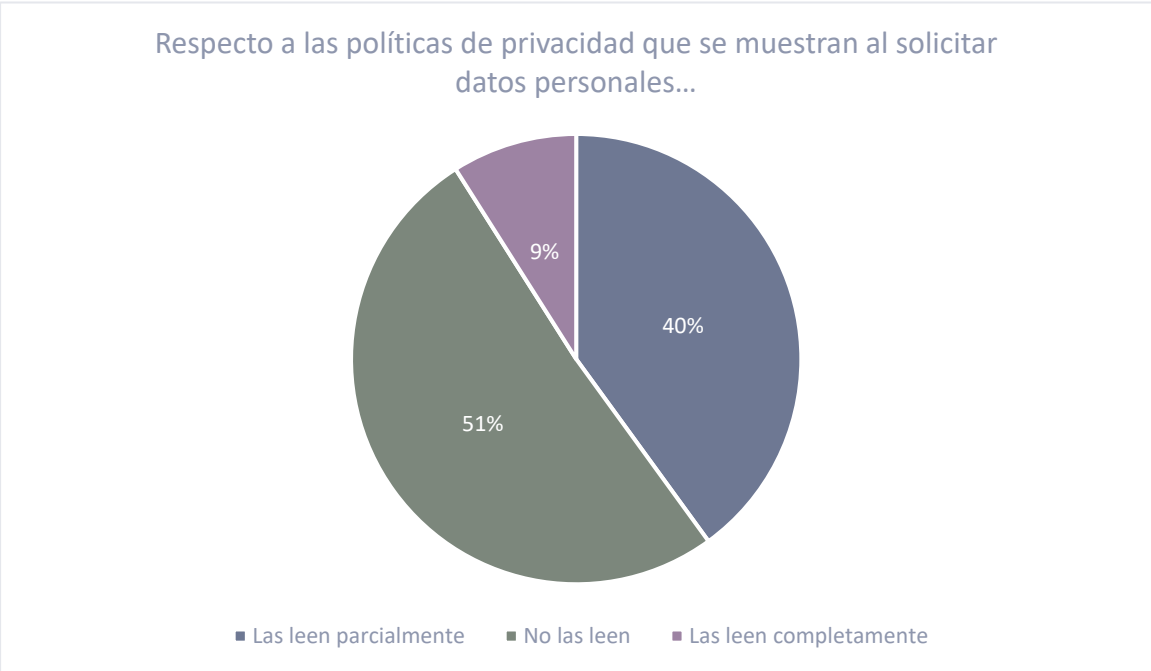

Figura 10: Elaboración propia

Otro aspecto relevante sería por qué los internautas no leen estas políticas de privacidad: el motivo principal en todos los países de la UE es el hecho de ser excesivamente largas, siendo el segundo motivo habitualmente más citado (como en el caso de España) el hecho de que resulten poco claras o difíciles de comprender – opinión que comparte el 70% de los entrevistados por el CIS.

Teniendo en cuenta estos datos, se podría afirmar que la ciudadanía muestra una clara preocupación por su privacidad, pero resulta especialmente revelador el hecho de que algunas personas ya están intentando comprender cómo se tratan sus datos personales para actuar en consecuencia.

Las campañas de concienciación lanzadas desde las instituciones y organismos suponen un punto fuerte en la alianza entre los usuarios y el sistema.

A nivel de la UE, la Comisión Europea anima a los usuarios a leer las declaraciones de confidencialidad y optimizar sus opciones de privacidad, organizando en su página web una sección dedicada a las preguntas más frecuentes y dando respuestas fáciles y comprensibles.

En el ámbito español también se pueden encontrar varias iniciativas. En primer lugar, el Instituto Nacional de Ciberseguridad lanza campañas[166] de concienciación que explican de forma sencilla cuestiones relativas a las redes sociales, los dispositivos utilizados en el trabajo, los móviles, compras online, configuración de contraseñas...utilizando infografías o vídeos. Además, la Agencia Española de Protección de Datos destaca por su labor divulgativa a través de la publicación de numerosas Guías. En este caso, la Guía para el Ciudadano[167] es una muestra de la voluntad de la AEPD de orientar y dar luz no solo a entidades u organizaciones particulares sino también a la ciudadanía.

Google y la Organización de Consumidores y Usuarios, en colaboración con la AEPD y el Instituto Nacional de Ciberseguridad, han anunciado el lanzamiento de la segunda edición de su campaña *Vive un Internet seguro* cuya finalidad es continuar informando a los internautas y darles las herramientas necesarias para asegurar su protección en materia de privacidad y seguridad en Internet, habilitando una plataforma[168] accesible y gratuita donde se puede encontrar una guía para padres y educadores, consejos, test...entre otros.

En el terreno autonómico, también la Generalitat Valenciana ha mostrado su compromiso con la concienciación elaborando, desde la Delegación de Protección de Datos, algunas recomendaciones entre las cuales podemos destacar la relativa al ejercicio del derecho de acceso[169]. Asimismo, el *Centre de Seguretat TIC de la Comunitat Valenciana* ha creado la plataforma *ConcienciaT*, en la cual se puede encontrar una gran variedad de infografías[170] referentes a cómo mantener la seguridad en distintos ámbitos: turismo, entornos sanitarios, uso de dispositivos IoT, etcétera.

Es por ello que, únicamente los usuarios, empoderados con herramientas y conocimiento necesario para conocer a qué se están destinando sus datos, podrán ser parte activa de esta relación con entidades y administraciones que tratan sus datos que, por su parte, deberán contribuir aplicando en sus prácticas la debida transparencia y respetando los debidos estándares éticos, legales y de seguridad desde el diseño y por defecto.

[166] N.B.: *Vid.* https://www.osi.es/es/campanas

[167] AEPD, *Protección de Datos: Guía para el Ciudadano*, mayo de 2020, https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

[168] N.B.: *Vid.* https://viveinternetseguro.org/?_ga=2.118806153.149690011.1569926083-363139414.1569926083

[169] GENERALITAT VALENCIANA, "Recomendación Ejercicio del Derecho de Acceso", Delegación de Protección de Datos GVA, 2019, http://participacio.gva.es/documents/166475129/167697765/Recomendaci%C3%B3n+2019%20001.+Ejercicio+del+Derecho+de+Acceso.pdf/ee4ed75c-196e-4366-9619-4a66c09e9662

[170] N.B.: *Vid.* https://concienciat.gva.es/infografias

Bibliografía

AENOR, "ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad", por Boris Delgado Riss y Carlos Manuel Fernández, mayo de 2019.Online: <https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html>.

AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, 2020, p. 5. Online: <https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf>.

AEPD, Código de buenas prácticas en protección de datos para proyectos Big Data, Coords.: Emilio Aced, M. Rosario Heras y Carlos Alberto Sáiz, 2019, pág 3. Online: <https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf>.

AEPD, Protección de Datos: Guía para el Ciudadano, mayo de 2020. Online: <https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf>.

APDCAT, Inteligencia Artificial: Decisiones Automatizadas en Cataluña, 2020, pág. 21. Online: <https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf>.

BARRIO, M., Internet de las Cosas. Madrid: Reus, 2018, pág. 21.

BEJERANO, P., "Diferencias entre machine learning y deep learning", Telefónica Think Big Empresas, 8 de febrero de 2017. Online: <https://blogthinkbig.com/diferencias-entre-machine-learning-y-deep-learning>.

CAPGEMINI RESEARCH INSTITUTE, "Reinventing Cybersecurity With Artificial Intelligence", 2019. Online: <https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/07/AI-in-Cybersecurity_Report_20190710_V05.pdf>.

CEPAL, Informe "La Nueva Revolución Digital: de la Internet del consumo a la Internet de la producción". Comisión Económica para América Latina y el Caribe, 2018, p. 36. Online: <https://repositorio.cepal.org/bitstream/handle/11362/38604/4/S1600780_es.pdf>.

CESE, "Inteligencia artificial: anticipar su impacto en el trabajo para garantizar una transición justa", Dictamen 2018/C 440/0, Comité Económico y Social Europeo, 6 de diciembre de 2018, p. 3.

CIS, Barómetro de mayo de 2018, estudio nº 3213. Online: <http://datos.cis.es/pdf/Es3213mar_A.pdf>.

COMISIÓN EUROPEA, A Definition of AI: Main capabilities and disciplines, por el grupo de expertos de alto nivel en Inteligencia Artificial, 2018, pág. 6. Online: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

COMISIÓN EUROPEA , "El momento de Europa: reparar los daños y preparar el futuro para la próxima generación", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 456 final, Online: <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0456/COM_COM(2020)0456_ES.pdf>.

COMISIÓN EUROPEA, Directrices éticas para una IA fiable, Grupo de expertos de alto nivel en Inteligencia Artificial, abril de 2019. Online: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

COMISIÓN EUROPEA, “Hacia una economía de los datos próspera”, Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM/2014/0442 final, 2 de julio de 2014. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014DC0442&from=ES>.

COMISIÓN EUROPEA, "High-Level Expert Group on Artificial Intelligence", Online: <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>.

COMISIÓN EUROPEA, “La construcción de una economía de los datos europea”, Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM (2017) 9 final, 10 de enero de 2017.

COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza, COM(2020) 65 final, 19 de febrero de 2020. Online: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf>.

COMISIÓN EUROPEA, “Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica”, Informe a la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, COM(2020) 64 final, 19 de febrero 2020. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064>.

COMISIÓN EUROPEA, “Inteligencia artificial para Europa”, Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2018) 237 final, 25 de abril de 2018. Online: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF>.

COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea, y se deroga el Reglamento (CE) nº 216/2008 del Parlamento Europeo y del Consejo, 2015/0277/COD, 7 de diciembre de 2015, artículo 3 (29).

COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), 2017/0003(COD), 10 de enero de 2017. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010>

COMISIÓN EUROPEA, “Una Estrategia Europea de Datos”, Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 66 final, 19 de febrero de 2020. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&from=ES>.

COMISIÓN EUROPEA, “Una Estrategia para el Mercado Único Digital de Europa”, Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2015) 192 final, 6 de mayo de 2015. Online: < https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=ES>.

COTINO HUESO, L., “Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho”, Revista General de Derecho Administrativo, nº50, 2019, p.7.

COMISIÓN EUROPEA, “487a. General Data Protection Regulation - 487b. Charter of Fundamental Rights”, Public Opinion, marzo de 2019. Online: <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222>.

CONSEJO DE EUROPA, "Algorithms and human rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications", Committee of experts on internet intermediaries (MSI-NET), 2018. Online: <https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>.

CONSEJO DE EUROPA, Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4 de noviembre de 1950.

CRAIG, T., LUDLOFF, M. E., Privacy and Big Data, O'Reilly, Sebastopol (CA), 2011

DGT, "Instrucción 15/V-113 sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general", Dirección General de Tráfico del Ministerio del Interior, p. 1. Online: <http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/15.V-113-Vehiculos-Conduccion-automatizada.pdf>.

DGT, "Instrucción 16 TV/89 sobre estacionamiento asistido de vehículos a motor", Dirección General de Tráfico del Ministerio del Interior, 20 de enero de 2016. Online: <http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/2016/Instruccion_16_TV_89_Estacionamiento_asistido_vehiculos_motor.pdf>.

EL PAÍS, "Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres", por Isabel Rubio, 12 de octubre de 2018. Online: <https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html>.

ENISA, Big Data Security Good Practices and Recommendations on the Security of Big Data Systems, diciembre de 2015. Online: <https://www.enisa.europa.eu/publications/big-data-security>.

ENISA, *Big Data Threat Landscape and Good Practice Guide,* enero de 2016. Online: <https://www.enisa.europa.eu/publications/bigdata-threat-landscape>.

ENISA, "Cloud Computing Certification - CCSL and CCSM". Online: <https://resilience.enisa.europa.eu/cloud-computing-certification>.

ESPAÑA, Constitución Española, BOE 29 de diciembre de 1978, artículo 55.

GENERALITAT VALENCIANA, "Recomendación Ejercicio del Derecho de Acceso", Delegación de Protección de Datos GVA, 2019. Online: <http://participacio.gva.es/documents/166475129/167697765/Recomendaci%C3%B3n+2019%20001.+Ejercicio+del+Derecho+de+Acceso.pdf/ee4ed75c-196e-4366-9619-4a66c09e9662>.

GOBIERNO DE ESPAÑA, Estrategia Española de I+D+i en Inteligencia Artificial, Ministerio de Ciencia, Innovación y Universidades, 2019. Online: <https://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pdf>.

GOÑI SEIN, J.L., Defendiendo los derechos fundamentales frente a la Inteligencia Artificial, Universidad de Navarra, lección de 13 de septiembre de 2019. Online: <https://www.unavarra.es/digitalAssets/244/244921_100000Leccion-inaugural-Castellano-19-20_web.pdf>.

GT29, Dictamen 8/2014 sobre la evolución reciente del Internet de los Objetos, elaborado por el Grupo de Trabajo sobre protección de datos del artículo 29 (Unión Europea), 16 septiembre de 2014, pág. 4. Online: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf>.

GUADAMUZ, A., "La inteligencia artificial y el derecho de autor", OMPI revista, octubre de 2017. Online: <https://www.wipo.int/wipo_magazine/es/2017/05/article_0003.html>.

HOFFMANN-RIEM, W., Big Data. Desafíos también para el Derecho, Pamplona: Civitas, 2018, pág. 51.

IEC. Artificial intelligence across industries. International Electrotechnical Comission Whitepaper. Online: <https://basecamp.iec.ch/download/iec-white-paper-artificial-intelligence-across-industries-en/>.

IEC, "ISO/IEC JTC 1/SC 41 Work programme". Online: <https://www.iec.ch/dyn/www/f?p=103:23:8187723854992::::FSP_ORG_ID,FSP_LANG_ID:20486,25>.

IDC RESEARCH ESPAÑA, "El Mercado de Internet de las Cosas en España". Online: <https://idcspain.com/research/IoTSpain>.

IMREI, K. (Ed.), "Data as the Engine of Europe's Digital Future", The European Data Market Monitoring Tool Report, junio de 2019, 51 págs. Online: <http://datalandscape.eu/sites/default/files/report/EDM_D2.5_Second_Report_on_Policy_Conclusions_final_13.06.2019.pdfZ>.

IoT ANALYTICS, IoT Platforms Company Landscape 2020. Online: <https://iot-analytics.com/product/iot-platforms-landscape-database-2020>.

ISO, "ISO/IEC JTC 1Information Technology", International Organization for Standardization. Online: <https://www.iso.org/isoiec-jtc-1.html>.

JUANES, C., DE FUENTES, J.M., SAN JOSÉ, J., "Ciberseguridad: Inteligencia artificial para garantizar la mejor defensa", Marketing y Ventas, núm. 161, mayo de 2020.

KALYANI, V.L., SHRAMA., D., "IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication", JMEIT, v. 2, nº. 6, diciembre de 2015. Online:

<http://www.jmeit.com/JMEIT%20Vol%202%20Issue%206%20Dec%202015/JMEITDEC0206003.pdf>.

LANEY, D., "3D Data Management: Controlling Data Volume, Velocity, and Variety", Application Delivery Strategies, META Group Inc, fichero 949, 6 de febrero de 2001, Online: <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>.

LOZA CORERA, M., "Big data e inteligencia artificial", Govertis Advisory Services, 4 de diciembre 2018. Online: <https://www.govertis.com/big-data-e-inteligencia-artificial>.

LOZA CORERA, M., "Hacia la economía de los datos europea: nuevo reglamento europeo 2018/1807", Govertis Advisory Services, 10 de diciembre de 2018. Online: <https://www.govertis.com/hacia-la-economia-de-los-datos-europea-nuevo-reglamento-europeo-2018-1807#_ftn3>.

LUCA, "¿Qué es la Inteligencia Artificial?", Diccionario Tecnológico. Online: <https://luca-d3.com/es/data-speaks/diccionario-tecnologico/inteligencia-artificial>.

MASHAW, J. L., "Prólogo", en: Recuerda Girela, M. A., Tecnologías disruptivas: Regulando el futuro, Aranzadi, Pamplona, págs. 41-43.

MAYER-SCHÖNBERGER, V., CUKIER, K., Big data. La revolución de los datos masivos, Madrid: Turner, 2013, pág. 22.

MERCADER UGUINA, J. R., "El futuro del trabajo y el empleo en la era de la digitalización y la robótica", En: DE LA QUADRA-SALCEDO, T., PIÑAR MAÑANAS, J. L. (Dirs.), Sociedad digital y Derecho, Madrid: BOE, 2018, pág. 617. Online: <https://www.boe.es/publicaciones/biblioteca_juridica/abrir_pdf.php?id=PUB-NT-2018-97>.

NACIONES UNIDAS, Declaración Universal de los Derechos Humanos, 217 (III) A. Paris, 1948.

NACIONES UNIDAS, Pacto Internacional de Derechos Civiles y Políticos. Resolución 2200 A (XXI) de la Asamblea General, 16 de diciembre de 1966.

NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", NISTIR 8228, junio de 2019. Online: <https://csrc.nist.gov/publications/detail/nistir/8228/final>.

PARLAMENTO EUROPEO, "El mercado único digital omnipresente", Fichas temáticas sobre la Unión Europea Parlamento Europeo. Online: <https://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente>.

PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 12 de septiembre de 2018, sobre los sistemas armamentísticos autónomos. Online: <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_ES.html>.

PÉREZ, C., "Aspectos legales del Big Data", Revista de Estadística y Sociedad, nº 68, 2016, p. 18.

PURDY. M, DAUGHERTY, P., Informe "Inteligencia Artificial, el futuro del crecimiento", Accenture, 2016, p. 4. Online: <https://www.accenture.com/cl-es/insight-artificial-intelligence-future-growth>.

PWC IDEAS, "Inteligencia artificial y Blockchain, el yin y el yang de la tecnología", 2016. Online: <https://ideas.pwc.es/archivos/20161111/inteligencia-artificial-y-blockchain-el-yin-y-el-yang-de-la-tecnologia>.

RABAH, K., "Convergence of AI, IoT, Big Data and Blockchain: A Review", The Lake Institute Journal, vol.1, núm.1, 2018, págs. 1-18.

RECUERO DE LOS SANTOS, P., "Tipos de aprendizaje en Machine Learning: supervisado y no supervisado", Telefónica Think Big Empresas, 16 de noviembre de 2017. Online: <https://empresas.blogthinkbig.com/que-algoritmo-elegir-en-ml-aprendizaje>.

RICHARDSON, R., SCHULTZ, J., CRAWFORD, K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," 94 N.Y.U. L. Rev. Online, nº 192, marzo 2019. Online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423>.

RODRÍGUEZ CANFRANC, P. et al., "Sociedad Digital en España 2019", Fundación Telefónica, abril 2020, pág. 28. Online: <https://www.fundaciontelefonica.com/noticias/informe-sociedad-digital-espana-2019>.

SAMOILI, S., LÓPEZ COBO, M., GÓMEZ, E., DE PRATO, G., MARTÍNEZ-PLUMED, F., & DELIPETREV, B., AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence, Luxembourg: Publications Office of the European Union, 2020, pág. 8. Online: <https://ec.europa.eu/jrc/en/publication/ai-watch-defining-artificial-intelligence>.

SÁNCHEZ CHINCHÓN, A., "Los algoritmos nos facilitan la vida: así funcionan", Telefónica Think Big Empresas, 21 de noviembre de 2016. Online: <https://empresas.blogthinkbig.com/los-algoritmos-nos-facilitan-la-vida-asi-funcionan>.

SANTAMARÍA RAMOS, F. J.: "Internet de las cosas: un desafío para la protección de datos personales", Actualidad Administrativa nº 7-8, julio-agosto 2015, págs. 40-57.

SCHNEIER, B., "Technologists vs. Policy Makers", IEEE Security & Privacy, vol. 18, January-February 2020, págs. 71-72.

THE GUARDIAN, "Rise of the racist robots – how AI is learning all our worst impulses", por Stephen Buranyi, 8 de agosto de 2017. Online:

<https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>

THE GUARDIAN, "The great British Brexit robbery: how our democracy was hijacked", por Carole Cadwalladr, 7 de mayo de 2017. Online: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>.

TRIBUNAL CONSTITUCIONAL, Sentencia 24/2019, de 25 de febrero, FJ 5. Online: <http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25869#complete_resolucion&fundamentos>.

TRIBUNAL CONSTITUCIONAL, Declaración inconstitucionalidad artículo 58bis LOPDGDD, vid. SENTENCIA 76/2019, de 22 de mayo. Online: <https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf>.

TSCHIDER, Ch., "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence", 96 Denv. U. L. Rev. 87 Age, marzo de 2018, pág. 120.

UNE, "Impulso español a las normas mundiales sobre IA, Big Data e IoT", por José Antonio Jiménez, La revista de la normalización española, enero de 2020. Online: <https://revista.une.org/21/impulso-espanol-a-las-normas-mundiales-sobre-ia-big-data-e-i.html>.

WEF, "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications", 2020. Online: <https://www.weforum.org/global-risks/reports>.

Sobre Telefónica Tech

Telefónica Tech es un holding de empresas propiedad del grupo Telefónica. La compañía cuenta con una amplia oferta de soluciones tecnológicas llegando a más de 5,5 millones de clientes en 175 países. Telefonica Tech podrá albergar otros negocios digitales a futuro, incluso del segmento B2C.

Más información

telefonicatech.com