

# **La sociedad del dato**

**Antonio L. Flores Galea**



***Revista Digital de ACTA***

***2024***

**Publicación patrocinada por**



**ACTA representa en CEDRO los intereses de los autores científico-técnicos y académicos. Ser socio de ACTA es gratuito.**

**Solicite su adhesión en [acta@acta.es](mailto:acta@acta.es)**

## **La sociedad del dato**

© 2024, **Antonio L. Flores Galea**

© 2024, 

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley.

Se autorizan los enlaces a este artículo.

*ACTA no se hace responsable de las opiniones personales reflejadas en este artículo.*

## INTRODUCCIÓN

En un mundo donde cada interacción digital genera datos y cada vez se realizan más interacciones digitales, la información se ha convertido en el recurso más valioso. Esta revolución, impulsada por el crecimiento de tecnologías como el Big Data, la inteligencia artificial y el Internet de las Cosas, ha permitido avances sin precedentes en prácticamente todos los sectores.

Sin embargo, este nuevo entorno está generando no solo una dependencia de los datos para el funcionamiento de los servicios al ciudadano y procesos de negocio, sino también para las interacciones sociales, ya sea mediante el uso de las redes sociales como los sistemas de opiniones y recomendaciones o los servicios de noticias.

La sociedad está entrando en una nueva fase donde el foco está pasando del individuo a su huella digital. El dato se vuelve más importante que la realidad y, en este ecosistema, el control y la manipulación de los datos se ha convertido en la meta de las grandes multinacionales, los gobiernos y también las personas y organizaciones con fines oscuros.

En este artículo, el autor acuña el concepto "sociedad del dato" en referencia a esta nueva realidad, desarrollando cómo se ha llegado a este punto, desgranando los pilares fundamentales sobre los que se articula la sociedad del dato y qué implicaciones puede tener en el futuro.

## LA SOCIEDAD DE LA INFORMACIÓN

La sociedad de la información es un concepto acuñado como consecuencia del auge de las tecnologías de la información y la comunicación (TIC) durante la segunda mitad del siglo XX, y representa la transición desde una sociedad industrial, centrada en la producción de bienes materiales, a una sociedad en la que el conocimiento y los servicios digitales son los principales motores de crecimiento. La evolución histórica de la sociedad de la información puede vincularse a diversos hitos tecnológicos y sociales, entre los que destacan:

- El desarrollo de Internet en las últimas décadas del siglo XX, que transformó la manera en que las personas acceden, procesan y distribuyen información.
- La digitalización generalizada de contenidos tradicionalmente disponibles en papel y de procesos y la creación de grandes plataformas tecnológicas globales que han permitido el acceso a grandes volúmenes de información y la interconexión de millones de personas por distintos mecanismos.
- El avance de la informática y la capacidad de cómputo y de representación de los ordenadores, teléfonos móviles y otros dispositivos, que ha facilitado su utilización generalizada para acceder a los contenidos digitalizados e interactuar con ellos de manera más cómoda y eficaz que en soporte papel.

El concepto de "sociedad de la información" fue ampliamente popularizado en la década de 1990, cuando organismos internacionales como la UNESCO y la Unión Internacional de Telecomunicaciones (UIT) comenzaron a utilizarlo para describir las profundas transformaciones impulsadas por la expansión de Internet y las TIC.

## POPULARIZACIÓN DURANTE LA DÉCADA DE 1990

La década de 1990 marcó un punto de inflexión para la popularización del concepto de la sociedad de la información. Este período fue testigo de avances tecnológicos clave y de un creciente reconocimiento de la importancia de las TIC en la transformación de la economía y la sociedad.

Probablemente el evento más significativo fue la expansión de Internet a escala global. Aunque Internet ya había sido desarrollada durante las décadas anteriores, fue durante los años noventa cuando se convirtió en un fenómeno de masas, facilitado por la creación de navegadores web que facilitaban el acceso y búsqueda de contenidos (como Netscape y, más tarde, Internet Explorer) y la creciente adopción de ordenadores personales en hogares y empresas. De esta forma, la World Wide Web (www) se convirtió en el principal medio para compartir y acceder a información, y surgieron las primeras páginas web comerciales y motores de búsqueda, como Yahoo! y Altavista, que transformaron la forma en que las personas interactuaban con la información.

En paralelo, instituciones internacionales comenzaron a reconocer y a definir formalmente el concepto de "sociedad de la información". La UE, por ejemplo, lanzó su iniciativa "Bangemann Report" en 1994, que subrayaba la necesidad de promover la infraestructura digital en Europa para competir en la economía global. La UIT también desempeñó un papel crucial al organizar la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en la que gobiernos, empresas y organizaciones no gubernamentales discutieron el potencial transformador de las TIC.

Además, en 1995, Nicholas Negroponte, director del MIT Media Lab, publicó el influyente libro "Being Digital", que destacó cómo la digitalización de la información estaba creando un nuevo entorno global en el que los bits (la unidad básica de información) sustituirían a los átomos (la materia física) como la principal forma de intercambio económico y cultural. Estas ideas influyeron en la comprensión popular y académica de la sociedad de la información, consolidando la idea de que el conocimiento y los datos serían el principal motor de crecimiento en el futuro.

En este contexto, la sociedad de la información se consolidó como un paradigma tanto en las políticas públicas como en los debates académicos. Los gobiernos comenzaron a desarrollar estrategias para fomentar la conectividad digital y preparar a sus economías y ciudadanos para las nuevas oportunidades que ofrecían las TIC.

## **IMPACTO EN LA COMUNICACIÓN Y LA ECONOMÍA GLOBAL**

La sociedad de la información transformó profundamente los patrones de comunicación a nivel global. Con la creciente accesibilidad a Internet, la comunicación pasó de ser una actividad limitada por la distancia geográfica a una interacción instantánea y global. Esta transformación afectó tanto a las interacciones personales como profesionales y se ha visto impulsada hasta ahora por tres cuestiones principales:

- **Acceso instantáneo a la información:** Gracias a Internet, ahora se tiene acceso inmediato a una vasta cantidad de información, desde noticias en tiempo real hasta bases de datos científicas, bibliotecas digitales e información procedente de sensores, vehículos, objetos, etc. Esto ha facilitado una comunicación más rápida y eficaz, habilitando a las personas a participar en foros y decisiones a escala mundial.
- **Redes sociales y colaboración global:** El auge de las redes sociales en la primera década del siglo XXI fue impulsado por la infraestructura desarrollada en la década de 1990. Plataformas como Facebook, X, Instagram y LinkedIn han transformado las relaciones personales y profesionales, permitiendo la creación de redes globales de colaboración y comunidad en tiempo real. La participación ciudadana en movimientos sociales y políticos ha ganado fuerza a través de estas plataformas, ya que las personas pueden compartir información, coordinar acciones y movilizarse de manera más eficiente, a la vez que los medios de comunicación y gobiernos las utilizan para transmitir sus mensajes e ideas de manera mucho más directa y eficaz.
- **Medios de comunicación:** Los medios tradicionales, como la televisión y los periódicos, han sido transformados por la digitalización. Hoy en día, los medios de comunicación

dependen cada vez más de plataformas digitales para la distribución de contenido. La proliferación de medios digitales ha democratizado el periodismo, permitiendo que ciudadanos de todo el mundo se conviertan en creadores de contenido, y facilitando el acceso a diversas perspectivas e informaciones.

En el plano económico, la sociedad de la información ha dado lugar a un nuevo paradigma en el que la información, los datos y el conocimiento son los principales motores de crecimiento económico. Este fenómeno ha reconfigurado profundamente la estructura de las economías globales, generando nuevas oportunidades, así como retos:

- **Economía basada en el conocimiento:** La transición hacia una economía basada en el conocimiento, que se analiza más adelante en este artículo, ha implicado que las industrias tradicionales basadas en la manufactura hayan sido desplazadas por otras centradas en la creación, distribución y gestión de datos y conocimiento. Sectores como el TIC, los servicios financieros, el marketing digital y la educación online han crecido de manera exponencial en las últimas décadas.
- **Digitalización y productividad:** La digitalización de procesos ha mejorado la eficiencia y productividad de las empresas en todo el mundo. La automatización de tareas mediante sistemas informáticos, el análisis de grandes volúmenes de datos (Big Data) y la utilización de inteligencia artificial han permitido a las empresas optimizar la toma de decisiones, reducir costes y desarrollar nuevos productos y servicios más rápidamente.
- **Nuevas industrias y puestos de trabajo:** La sociedad de la información ha dado lugar al surgimiento de nuevas industrias que dependen en gran medida de la gestión y el análisis de datos. Los sectores de desarrollo de software, análisis de datos, ciberseguridad y tecnología *blockchain* son ejemplos de campos que se han creado o han crecido en importancia y que ofrecen bastantes oportunidades laborales en el marco de esta nueva economía. Al mismo tiempo, se han creado nuevas profesiones, como la de "científico de datos", "ingeniero de IA" o "*community manager*", entre otras.
- **Concentración del poder económico:** Sin embargo, el surgimiento de la economía digital también ha planteado retos importantes. Las empresas que controlan la infraestructura digital y los datos (como Google, Amazon, Facebook y Apple) han acumulado un poder económico sin precedentes, creando monopolios digitales que dominan sectores claves de la economía. Esta concentración de poder ha generado preocupaciones sobre la competencia y la regulación en el entorno digital que a día de hoy se encuentran sin resolver.
- **Brecha digital y desigualdades:** A pesar de haber aportado un crecimiento general, medido en promedio, la sociedad de la información ha causado la conocida "brecha digital", que se traduce en una amplificación de la brecha socioeconómica entre quienes tienen acceso a las tecnologías y quienes no. Las regiones y poblaciones con menos acceso a Internet, infraestructura tecnológica o habilidades digitales se enfrentan a retos cada vez más difíciles de superar para participar en la economía global, lo que genera nuevas desigualdades y miseria en determinadas zonas o estratos sociales.
- **Globalización y mercados digitales:** Finalmente, la digitalización ha facilitado la globalización de los mercados. Empresas y emprendedores de todo el mundo pueden ahora acceder a consumidores globales a través de plataformas de comercio electrónico, lo que ha permitido la creación de mercados digitales globales ("*digital marketplaces*"). Sin embargo, esta globalización también supone un problema para las pequeñas y medianas empresas locales, que no pueden competir con las grandes multinacionales, a la vez que el fenómeno de la globalización continúa desdibujando la cultura local para imponer valores y gustos globales, generalmente heredados del mundo anglosajón, que producen una alienación y homogeneización de todas las personas en pro de una búsqueda de mayores economías de escala y beneficios económicos para estas multinacionales, que consiguen ampliar su mercado con productos estándares globales.

## DEMOCRATIZACIÓN DE INTERNET

Otro concepto asociado a la sociedad del conocimiento y uno de los pilares básicos de la sociedad del dato es la democratización de Internet. Se refiere al proceso mediante el cual el acceso a la información, el conocimiento y las herramientas tecnológicas se ha vuelto más accesible para un número creciente de personas en todo el mundo. Desde su creación, Internet ha pasado de ser una herramienta restringida a instituciones académicas y gubernamentales a un recurso global al alcance de miles de millones de personas.

Durante la década de 1990, Internet comenzó a expandirse más allá del ámbito militar y académico, gracias a la creación de la WWW y de los primeros navegadores que facilitaron el acceso a información online. Sin embargo, en esta etapa temprana, el acceso a Internet estaba limitado principalmente a países desarrollados y a personas con formación técnica o académica y sus aplicaciones eran muy limitadas, pues el tipo de información que manejaba era reducida y muy especializada dentro de estos campos.

Sin embargo, con el abaratamiento del coste de las telecomunicaciones y nuevas tecnologías de transmisión de datos como el ADSL y, posteriormente, la fibra óptica, así como la creciente disponibilidad de dispositivos como ordenadores personales y, posteriormente, teléfonos inteligentes en los hogares, Internet empezó a llegar a más sectores de la población y a regiones en desarrollo. Así, durante la primera década del siglo XX, la expansión de las redes de banda ancha y la aparición de las redes sociales consolidaron la presencia de Internet como una parte fundamental de la vida cotidiana.

En la actualidad, más de la mitad de la población mundial tiene acceso a Internet. Este crecimiento se debe fundamentalmente al abaratamiento y expansión de las infraestructuras de telecomunicaciones, la disminución de los costes de acceso a dispositivos de acceso (ordenadores, tabletas y smartphones) y las políticas gubernamentales destinadas a promover el acceso a Internet y el uso de servicios digitales, especialmente aceleradas durante la pandemia de COVID. La aparición de tecnologías móviles y redes 4G y 5G ha permitido que muchas personas en áreas rurales o en países en desarrollo puedan acceder a Internet por primera vez, lo que representa un hito importante en la democratización del acceso a la información.

No obstante, aún persisten retos importantes para garantizar que Internet esté verdaderamente disponible para todos. La infraestructura no es ni mucho menos igual de accesible en todas las partes del mundo, y los costes de acceso a los dispositivos y servicios de conectividad siguen siendo prohibitivos en muchos países y para ciertos estratos sociales, teniendo en cuenta su renta per cápita, lo que se denomina, como ya se ha adelantado, la "brecha digital".

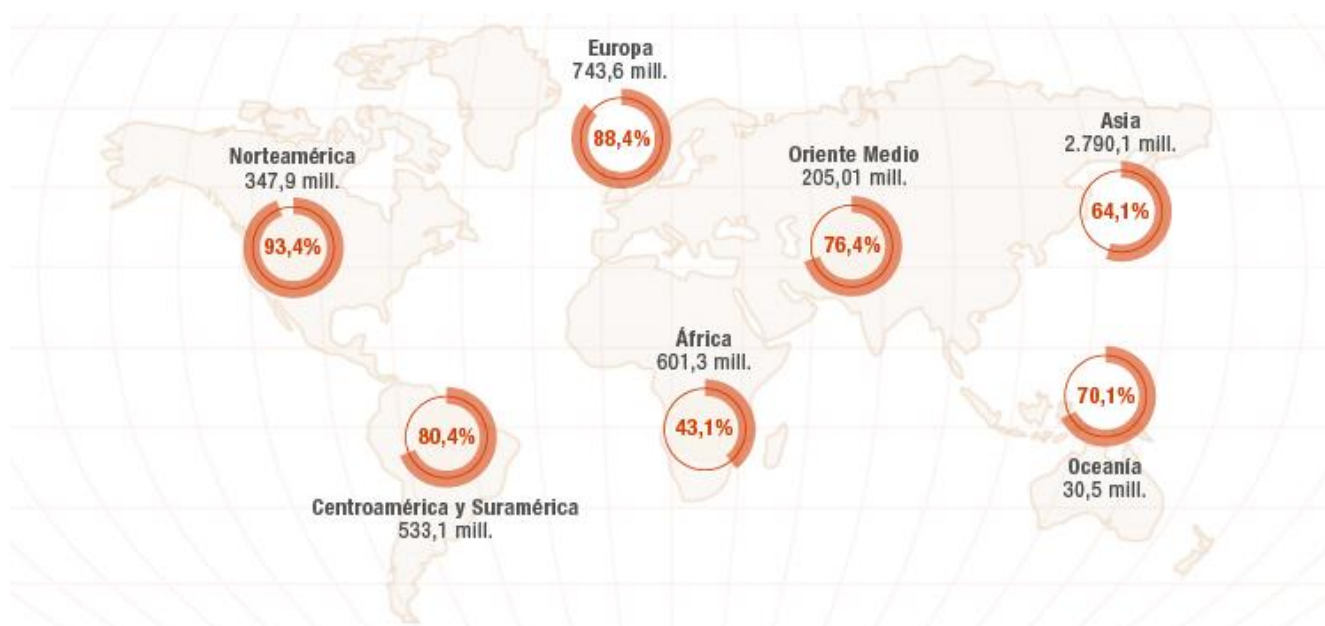
## BRECHA DIGITAL: RETOS PARA LA EQUIDAD TECNOLÓGICA

A pesar del progreso en la expansión del acceso a Internet, existe una brecha digital que continúa separando a las personas que tienen acceso a tecnologías digitales de las que no lo tienen. Esta brecha no solo está relacionada con el acceso físico a Internet, sino también con factores sociales, económicos y educativos, como ya se ha indicado. Las causas de la brecha digital pueden ser resumidas en las siguientes categorías:

- **Geográficas:** La brecha digital es particularmente evidente en las zonas rurales y en los países en desarrollo, donde la infraestructura para el acceso a Internet es menos avanzada por los mayores costes de despliegue y menores economías de escala debidas a la menor densidad de población o capacidad de gasto. Mientras que en los países desarrollados más del 80% de la población tiene acceso a Internet, en regiones como el África subsahariana

la penetración de Internet aún está por debajo del 30%. Esta disparidad geográfica tiene implicaciones significativas, ya que las comunidades sin acceso a Internet carecen de oportunidades para acceder a la educación, servicios de salud, comercio electrónico y otras formas de desarrollo económico.

- **Socioeconomía:** El coste del acceso a Internet sigue siendo un obstáculo importante para muchas personas. Los precios de los dispositivos y los planes de datos son relativamente altos en comparación con los ingresos promedio en muchos países en desarrollo. Además, las personas con ingresos bajos en los países desarrollados también pueden tener dificultades económicas para acceder a Internet de manera regular o con una conexión de calidad para utilizar determinados servicios. Esta situación perpetúa la desigualdad, ya que las oportunidades que ofrece Internet (por ejemplo, en educación y oportunidades de empleo) serán más accesibles a quienes tengan mayores recursos económicos.
- **Educación y habilidades digitales:** La falta de conocimientos técnicos y habilidades digitales también contribuye a la brecha digital. Aunque el acceso a dispositivos e Internet se ha extendido, no todas las personas tienen las competencias necesarias para utilizar plenamente las tecnologías digitales. En este sentido, la alfabetización digital se ha convertido en una nueva forma de capital cultural que determina las oportunidades y el éxito en la sociedad actual.
- **Género:** Existe también una brecha de género en el acceso y uso de Internet. En muchas partes del mundo, ya sea debido a cuestiones culturales o religiosas, las mujeres tienen menos acceso a dispositivos tecnológicos y a la red que los hombres. Esta desigualdad tecnológica refleja y refuerza otras desigualdades de género en el ámbito socioeconómico, limitando el acceso de las mujeres a oportunidades educativas, laborales y de interacción social.



**Figura 1. Tasa de penetración y número de usuarios de Internet en el mundo en diciembre de 2021**  
(Fuente: Internet World Stats)

Para reducir la brecha digital, los gobiernos y algunas organizaciones no gubernamentales han ido implementando iniciativas para extender el acceso a Internet y fomentar la alfabetización digital. Algunos ejemplos son el programa "Internet para Todos" de la UIT y los esfuerzos de empresas tecnológicas, como Google, Facebook y Starlink, para llevar Internet a áreas remotas mediante tecnologías innovadoras, como globos estratosféricos, drones y satélites, respectivamente.

## PARTICIPACIÓN CIUDADANA Y ACCESO A LOS DATOS

La democratización de Internet también ha tenido un impacto profundo en la participación ciudadana y en el acceso a los datos, lo que ha transformado las formas en que las personas interactúan con sus gobiernos, instituciones y entre ellas mismas. Se pueden destacar las siguientes iniciativas:

- **Participación en la vida pública:** Internet ha facilitado una mayor participación ciudadana en la vida política y social. Plataformas como redes sociales y blogs han dado a los individuos voz en debates públicos que antes eran dominados por los medios tradicionales. En muchos casos, Internet ha servido como plataforma para movilizaciones sociales y políticas, como se vio durante las “primaveras árabes” o en movimientos recientes como el “black lives matter”. A través de Internet, los ciudadanos pueden organizarse, compartir información y exigir rendición de cuentas de sus líderes. Algunas instituciones incluso han lanzado iniciativas para que los ciudadanos expresen su opinión sobre determinados temas e iniciativas reguladoras, como la UE mediante el portal “Díganos lo que piensa” (“*Have your say*”, en inglés)\*.
- **Gobernanza abierta:** La generalización del acceso a Internet ha fomentado que los gobiernos hagan públicos datos para promover la transparencia y permitir que los ciudadanos participen activamente en la toma de decisiones, lo que se conoce como “gobernanza abierta”. Estos datos pueden ser de presupuestos, políticas públicas y estadísticas económicas o de uso de los servicios públicos, por ejemplo, lo que facilita el control y la auditoría por parte de la sociedad civil. Esta tendencia ha sido particularmente fuerte en países como Estados Unidos, donde se lanzó la iniciativa Data.gov, y en la UE, con su política de acceso abierto a los datos gubernamentales.
- **Periodismo ciudadano y verificación de datos:** El acceso generalizado a Internet ha permitido que cualquier persona pueda convertirse en creador de contenido e, incluso, periodista. El periodismo ciudadano ha florecido en plataformas como X y YouTube, donde personas corrientes pueden informar y retransmitir en tiempo real sobre sucesos en todo el mundo. Sin embargo, esto plantea retos para la verificación de la información, ya que la desinformación y las noticias falsas se difunden con gran facilidad en las redes sociales. En respuesta, han surgido iniciativas para verificar la autenticidad de los datos y luchar contra la manipulación informativa, las conocidas agencias de “*fact check*” o “verificadores de la verdad”, de las que se hablará más adelante, al describir la “sociedad del dato”.
- **Acceso a los datos como derecho:** En muchas partes del mundo, el acceso a Internet y a la información se está reconociendo como un derecho fundamental. En 2016, la ONU declaró que el acceso a Internet es esencial para el ejercicio de los derechos humanos, argumentando que la información y la comunicación son componentes esenciales para la libertad de expresión, la educación y la participación en la vida pública. Este reconocimiento ha impulsado políticas públicas destinadas a garantizar un acceso equitativo y universal a Internet.
- **Protección de los datos:** A pesar de sus ventajas, la democratización del acceso a los datos también plantea el importante reto de protegerlos, sobre todo en una sociedad cada vez más dependiente de ellos. El uso de datos personales por parte de empresas y gobiernos ha generado debates sobre la privacidad y el consentimiento explícito. La regulación de estos aspectos se ha convertido en una prioridad para las instituciones internacionales, como se observa en el Reglamento General de Protección de Datos (GDPR) de la UE, que

---

\* [https://ec.europa.eu/info/law/better-regulation/have-your-say\\_es](https://ec.europa.eu/info/law/better-regulation/have-your-say_es)



busca garantizar la transparencia en el uso de los datos personales y la protección de los derechos de los usuarios.

## LA SOCIEDAD DEL CONOCIMIENTO

Con posterioridad al concepto de "sociedad de la información", se forjó uno nuevo: la "sociedad del conocimiento". Este hace referencia a un estadio avanzado de desarrollo social y económico, en el que la capacidad para generar, procesar y aplicar conocimiento se convierte en el principal motor de la economía y el crecimiento. Aunque está relacionada con la sociedad de la información, la sociedad del conocimiento va un paso más allá, destacando el valor del conocimiento procesado y su aplicación en lugar del mero acceso a la información. Se puede afirmar que, para que pueda darse la sociedad del conocimiento, es necesaria cierta madurez en la sociedad de la información; en particular, que se haya producido una verdadera democratización del uso de Internet y que, en consecuencia, exista suficiente información disponible online para poder desarrollar una economía y sociedad basadas en tal información.

Es conveniente destacar que el conocimiento es el resultado de interpretar, analizar y aplicar la información para resolver problemas, innovar o tomar decisiones informadas. Es un recurso estratégico, ya que implica no solo tener datos disponibles, sino también la capacidad de utilizarlos de manera crítica y efectiva. En la sociedad del conocimiento, lo importante no es solo acumular información, sino transformarla en conocimiento útil. Las personas, las empresas y las instituciones que pueden hacer este proceso de conversión de manera eficaz se vuelven más competitivas y productivas. El conocimiento es esencial en sectores como la ciencia, la educación, la tecnología y la innovación, donde la habilidad para generar nuevas ideas y productos marca la diferencia.

El avance hacia una sociedad del conocimiento ha sido posible gracias a la proliferación de herramientas tecnológicas que permiten un acceso más rápido y fácil a la información, como motores de búsqueda avanzados, plataformas de aprendizaje online y sistemas de inteligencia artificial. Estas tecnologías facilitan la creación de redes de colaboración global y la distribución de conocimiento en tiempo real.

## PAPEL DE LA EDUCACIÓN Y EL APRENDIZAJE EN LA ERA DIGITAL

La educación y el aprendizaje desempeñan un papel fundamental en la sociedad del conocimiento. La capacidad de una sociedad para prosperar en este entorno depende en gran medida de su sistema educativo y de las oportunidades de aprendizaje continuo que ofrece a sus ciudadanos. En la era digital, la educación ha experimentado transformaciones profundas, impulsadas por la tecnología y las necesidades cambiantes del mercado laboral.

### Transformación de los sistemas educativos

Los sistemas educativos han tenido que adaptarse a las nuevas demandas de la sociedad del conocimiento. Las habilidades tradicionales, como la memorización de datos, han sido superadas por la necesidad de desarrollar otras competencias, como el pensamiento crítico, la resolución de problemas, la creatividad y la capacidad para aprender de manera autónoma. En este sentido, se ha pasado de una enseñanza centrada en la transmisión de información a un enfoque que promueve el aprendizaje activo y la construcción de conocimiento.

Se pueden distinguir dos bases de desarrollo de los nuevos modelos educativos:

- **Educación basada en proyectos:** En lugar de centrarse en la mera acumulación de información, muchos sistemas educativos están adoptando un enfoque de aprendizaje

basado en proyectos, en el que los estudiantes trabajan en problemas reales, desarrollan soluciones y aplican el conocimiento de manera práctica. Este modelo fomenta la colaboración, la investigación y la innovación, habilidades clave en la sociedad del conocimiento.

- **Integración de la tecnología en el aula:** Las tecnologías digitales han transformado la manera en que los estudiantes aprenden y los maestros enseñan. Plataformas de aprendizaje online, como Moodle, Canvas o BlackBoard, permiten a los estudiantes acceder a contenido educativo desde cualquier dispositivo. Además, herramientas como las pizarras interactivas, el aprendizaje a través de simulaciones y la realidad aumentada están enriqueciendo la experiencia educativa al hacer que el aprendizaje sea más dinámico y participativo.

### Aprendizaje a lo largo de la vida (*lifelong learning*)

En la sociedad del conocimiento, el aprendizaje no se detiene con la finalización de la educación formal. Dado el ritmo acelerado de los avances tecnológicos y el cambio constante en las demandas del mercado laboral, las personas deben estar preparadas para aprender nuevas habilidades a lo largo de su vida. Este concepto, conocido como *lifelong learning*, implica una educación continua, flexible y adaptable a las necesidades del individuo y de la sociedad.

- **Cursos en línea y educación a distancia:** La digitalización ha permitido que las personas puedan acceder a educación de calidad sin importar su ubicación geográfica. Los "cursos masivos abiertos online" (MOOC, por sus siglas en inglés) como los disponibles en plataformas como Coursera y Udemy, y también en YouTube, han revolucionado el acceso a la educación, permitiendo a personas de todo el mundo aprender sobre una amplia variedad de temas. Esto no solo ha democratizado el acceso al conocimiento, sino que también ha permitido a las personas mejorar sus habilidades profesionales de manera autónoma y a su propio ritmo.
- **Desarrollo de habilidades digitales:** Dado que la economía del conocimiento está impulsada en gran parte por la tecnología, la capacidad de utilizar herramientas digitales es esencial. La educación y la capacitación en competencias digitales (como la programación, la gestión de datos y la inteligencia artificial) se han convertido en pilares fundamentales para preparar a las personas para el mercado laboral de la era digital.

### Innovación en la enseñanza y el aprendizaje

La tecnología no solo ha cambiado lo que se enseña, sino también cómo se enseña. Innovaciones como la inteligencia artificial, la realidad virtual y aumentada y el análisis de datos educativos están permitiendo que los profesores personalicen el aprendizaje en función de las necesidades individuales de cada estudiante. En lugar de una enseñanza homogénea, los sistemas educativos ahora pueden ofrecer experiencias de aprendizaje más adaptadas a las fortalezas y debilidades de cada estudiante, mejorando así los resultados académicos y fomentando un aprendizaje más eficaz.

- **Inteligencia artificial en la educación:** Cada vez se van incorporando más herramientas de IA para identificar los patrones de aprendizaje de los estudiantes y ofrecer recomendaciones personalizadas. Estas plataformas pueden ayudar a los maestros a identificar qué áreas necesitan más atención y adaptar los planes de estudio en consecuencia. Por ejemplo, plataformas como Smart Sparrow utilizan IA para crear entornos de aprendizaje adaptativos que responden a las interacciones de los estudiantes.
- **Gamificación:** La gamificación, o el uso de elementos propios de los juegos en entornos de aprendizaje, se ha convertido en una herramienta bastante popular para motivar a los estudiantes y hacer que el aprendizaje sea más interactivo y atractivo. Al incorporar

juegos y retos en el proceso educativo se incentiva la participación activa y se mejora la retención de conocimiento.

## La educación como motor de la innovación

La sociedad del conocimiento también ha puesto un fuerte énfasis en la innovación como motor para el desarrollo económico y social. Las universidades, centros de investigación e instituciones educativas en general desempeñan un papel fundamental en la creación y difusión de conocimiento, así como en la formación de individuos capaces de generar nuevas ideas, productos y servicios. En muchas economías avanzadas, las instituciones educativas están profundamente integradas con la industria, promoviendo la investigación aplicada y la colaboración en proyectos innovadores.

- **Incubadoras y aceleradoras universitarias:** Muchas universidades han establecido incubadoras y aceleradoras que ayudan a los estudiantes y académicos a desarrollar y comercializar sus ideas. Estos programas brindan apoyo financiero, mentoría y acceso a redes de inversores y socios comerciales. Ejemplos notables son las incubadoras tecnológicas de universidades como el MIT y Stanford en EE. UU., que han ayudado a lanzar algunas de las empresas tecnológicas más innovadoras del mundo.
- **Transferencia de conocimiento:** El proceso de transferencia de conocimiento entre las universidades y las empresas ha adquirido una importancia crucial en la sociedad del conocimiento. A través de patentes, acuerdos de licencia y colaboraciones industriales, las universidades están contribuyendo activamente al desarrollo económico y al progreso social, transfiriendo las ideas y descubrimientos de la investigación académica al mercado.

## BIG DATA

Otro de los conceptos habilitadores de la sociedad del dato es el Big Data, que hace referencia a la recopilación, gestión y análisis de enormes volúmenes de datos que no pueden ser procesados utilizando métodos tradicionales. Estos datos pueden ser estructurados, como bases de datos organizadas, o no estructurados, como imágenes, videos y publicaciones en redes sociales. El concepto de Big Data no solo implica que la cantidad de datos a procesar sea elevada, sino también que estos datos sean heterogéneos y sea necesario procesarlos en un corto espacio de tiempo. Por eso, el Big Data se caracteriza por las conocidas "tres uves" (volumen, variedad y velocidad):

- **Volumen:** Una cantidad masiva de datos generados por las actividades digitales diarias, como transacciones comerciales, interacciones en redes sociales, dispositivos IoT y sensores industriales.
- **Variedad:** Que los datos no procedan de una sola fuente y que puedan ser de diversos tipos: desde texto y números hasta imágenes, videos, audio y datos de sensores. Estos datos se almacenan en múltiples formatos, lo que hace que su procesamiento y análisis sea complejo.
- **Velocidad:** Que los datos se generen y deban ser procesados en tiempo real o casi en tiempo real. La capacidad para procesar grandes volúmenes de datos de manera rápida es esencial para obtener información relevante a tiempo.

La importancia del Big Data radica en su capacidad para transformar enormes volúmenes de datos en información valiosa. Organizaciones en todo el mundo, tanto del sector público como privado, aprovechan el Big Data para identificar patrones, prever comportamientos futuros y tomar decisiones informadas. Esto les permite mejorar la eficiencia, personalizar servicios, innovar en productos

y reducir riesgos. En resumen, el Big Data ofrece una ventaja competitiva significativa al posibilitar un análisis profundo que conduce a mejoras operativas y oportunidades de negocio.

## **PRINCIPALES APLICACIONES DEL BIG DATA**

El Big Data tiene aplicación en diversos sectores, transformando la forma en que se opera y se genera valor. En el sector salud, por ejemplo, permite el desarrollo de la medicina personalizada, donde los tratamientos se adaptan a las características específicas de cada paciente a través del análisis de grandes volúmenes de datos genéticos y clínicos. Además, se utiliza para predecir la aparición de epidemias y optimizar la gestión de recursos hospitalarios.

En el sector financiero, el Big Data es clave para la detección de fraudes, ya que los algoritmos analizan transacciones en tiempo real para identificar patrones sospechosos. Asimismo, se emplea para mejorar la gestión de riesgos y hacer evaluaciones más precisas sobre la solvencia crediticia de los clientes. Además, el análisis de datos de los mercados financieros permite prever fluctuaciones, lo que influye en la toma de decisiones de inversión.

En el campo del marketing, el Big Data permite la personalización de campañas publicitarias basadas en los hábitos de consumo y el comportamiento de los usuarios. Esto optimiza el rendimiento de la publicidad al dirigirse a audiencias específicas. Las marcas también pueden analizar el sentimiento de los consumidores en redes sociales, ajustando sus estrategias de acuerdo con las opiniones y comentarios que reciben. De manera similar, el análisis de grandes volúmenes de datos permite una segmentación de mercado más precisa, adaptando productos y servicios a las preferencias de los diferentes grupos de clientes.

Y en el comercio tradicional, el Big Data se utiliza para mejorar la gestión de inventarios, asegurando que los productos estén disponibles en el lugar y momento adecuados. También permite prever la demanda de productos basándose en datos históricos y factores externos, optimizando así la planificación de la producción y distribución. Finalmente, en la industria energética, las soluciones de Big Data ayudan a optimizar el consumo energético, analizando datos de sensores y medidores inteligentes en tiempo real. Además, permite predecir fallos en infraestructuras críticas, facilitando el mantenimiento preventivo y mejorando la seguridad de las redes energéticas.

## **LA PRIVACIDAD Y SEGURIDAD DE LOS DATOS**

A pesar de los beneficios que ofrece el Big Data, su uso plantea importantes riesgos y desafíos, particularmente en lo que respecta a la privacidad y seguridad de los datos. Uno de los mayores retos es la protección de la privacidad, ya que la recolección masiva de información personal por parte de empresas y gobiernos puede derivar en un uso indebido de los datos. En muchos casos, los datos incluyen información confidencial, como detalles financieros o datos médicos y los usuarios no tienen control sobre cómo se utiliza esta información ni con quién se comparte. Para abordar este problema, muchas regiones han implementado regulaciones como el Reglamento General de Protección de Datos (GDPR) en la UE, que establece normas estrictas sobre la recolección, almacenamiento y uso de datos personales. Sin embargo, la protección de la privacidad sigue siendo un reto debido a la posibilidad de que datos anónimos puedan reidentificarse cuando se combinan con otros conjuntos de datos, especialmente con la ayuda de la IA.

Otro riesgo significativo es la seguridad de los datos. Almacenar grandes volúmenes de información en centros de datos y servidores crea vulnerabilidades que pueden ser explotadas mediante ciberataques. Las brechas de seguridad pueden resultar en la exposición de información sensible, lo que acarrea consecuencias económicas y reputacionales graves para las organizaciones. Para mitigar estos riesgos, las empresas deben invertir en infraestructuras de ciberseguridad robustas y

utilizar tecnologías de cifrado para proteger los datos. Sin embargo, a medida que los ciberdelincuentes desarrollan métodos más sofisticados, garantizar la seguridad de los datos es un reto constante.

Finalmente, un desafío adicional es el potencial de sesgo en los datos procesados. Si los datos utilizados para alimentar los algoritmos de análisis no son representativos o contienen errores, los resultados derivados de ellos pueden estar sesgados. Esto puede dar lugar a decisiones injustas o incorrectas, afectando áreas como la concesión de créditos, la selección de personal o el acceso a servicios. La calidad y representatividad de los datos es crucial para evitar estos problemas y garantizar que el Big Data se utilice de manera ética y justa.

## INTERNET DE LAS COSAS (IOT)

El Internet de las Cosas (IoT, por sus siglas en inglés) es un concepto que describe la interconexión de objetos físicos con Internet, permitiendo que estos dispositivos recopilen, compartan y actúen sobre datos sin intervención humana directa. Estos objetos pueden incluir desde electrodomésticos y automóviles hasta máquinas industriales y dispositivos médicos, que están equipados con sensores, software y tecnologías que les permiten comunicarse entre sí y con otros sistemas a través de la red. En términos simples, el IoT convierte a los objetos cotidianos en "inteligentes" mediante su integración con la tecnología digital.

El término IoT fue popularizado a fines de la década de 1990, aunque el concepto subyacente ya existía con la evolución de redes de sensores y tecnologías de comunicación. La verdadera expansión del IoT comenzó en la primera década del siglo XXI, con el desarrollo de redes inalámbricas más rápidas, sensores más económicos y accesibles, y la proliferación de dispositivos móviles y sistemas conectados. Un hito clave en su evolución fue la llegada de la conectividad 4G y, más recientemente, 5G, que ha permitido que los dispositivos IoT se comuniquen de manera más rápida y eficiente.

La evolución del IoT ha estado impulsada por la necesidad de automatización y optimización en sectores como la industria, la salud, el transporte y los hogares. Hoy en día, el IoT se ha expandido considerablemente, conectando miles de millones de dispositivos en todo el mundo, desde termostatos inteligentes y cerraduras de puertas hasta maquinaria industrial conectada en fábricas. Con el avance de las telecomunicaciones, como las redes 5G y la computación en la nube, el IoT continúa creciendo rápidamente, con el potencial de transformar aún más aspectos de la vida cotidiana y los procesos industriales.

## IMPACTO DEL IOT EN LA VIDA COTIDIANA Y EN LA INDUSTRIA

En el ámbito de la vida cotidiana, el IoT ha dado lugar al llamado "hogar digital", donde una variedad de dispositivos conectados, como termostatos, sistemas de iluminación, cámaras de seguridad y electrodomésticos, pueden ser controlados y monitorizados a distancia a través de smartphones o asistentes virtuales. Esto no solo ha mejorado la comodidad y eficiencia, sino que también ha permitido una mayor personalización en el uso de la tecnología en el entorno doméstico. Los vehículos también se han visto transformados por el IoT, incorporando capacidades de conectividad, lo que permite una navegación más eficaz, diagnósticos automáticos y, en algunos casos, conducción autónoma.

En el sector de la salud, el IoT ha permitido el desarrollo de dispositivos de monitorización remota que pueden vigilar el estado de salud de los pacientes en tiempo real. Esto es particularmente útil para pacientes con enfermedades crónicas, que pueden recibir atención continua sin la necesidad de visitas frecuentes al hospital. Los dispositivos portátiles, como los relojes inteligentes, también

forman parte del ecosistema IoT, ayudando a las personas a monitorizar su actividad física, frecuencia cardíaca y otros indicadores de salud.

Sin embargo, el impacto del IoT en la industria es quizás uno de los más significativos. En las fábricas, el IoT ha impulsado el desarrollo de fábricas inteligentes ("smart factories", en inglés), donde las máquinas y los equipos están conectados a través de redes para optimizar los procesos de producción. Sensores integrados en las máquinas pueden recopilar datos en tiempo real sobre su rendimiento y estado, lo que permite a las empresas predecir fallos, reducir el tiempo de inactividad y mejorar la eficiencia operativa. Esta automatización ha permitido a las empresas reducir costes, aumentar la productividad y mejorar la calidad del producto final.

En el sector energético, el IoT facilita la gestión inteligente de redes eléctricas, permitiendo un mejor control y medición del consumo energético en tiempo real. Esto ayuda a optimizar la distribución de energía y a reducir el desperdicio, especialmente en el contexto de la integración de fuentes de energía renovable. Además, en el transporte, el IoT ha transformado la logística mediante el seguimiento en tiempo real de flotas de vehículos, lo que permite una gestión más eficiente del transporte de mercancías, reduciendo también los costes y mejorando la puntualidad.

Otro sector que se ha visto beneficiado por el IoT es el agroalimentario, donde la agricultura inteligente utiliza sensores para monitorizar el suelo, las condiciones meteorológicas y el rendimiento de los cultivos. Esto permite a los agricultores optimizar el uso del agua, fertilizantes y pesticidas, lo que se traduce en una mayor productividad agrícola y un menor impacto ambiental.

## **RETOS EN SEGURIDAD Y GESTIÓN DE DATOS**

A pesar de las múltiples ventajas del IoT, existen retos importantes relacionados con la seguridad y la gestión de datos. Uno de los principales problemas de seguridad es que cada dispositivo IoT conectado representa un posible punto de entrada para los ciberataques. Muchos de estos dispositivos, especialmente los de bajo coste, debido a sus limitaciones de recursos y capacidad de cómputo, carecen de medidas de seguridad robustas, lo que los hace vulnerables a la manipulación y ciberataques. Además, como la cantidad de dispositivos conectados sigue creciendo exponencialmente, también aumenta la superficie de ataque para posibles intrusiones.

Los ciberataques en el IoT pueden tener consecuencias graves, como el robo de datos personales, el control remoto de dispositivos domésticos o industriales, o la interrupción de servicios críticos. Por ejemplo, un ataque a una red eléctrica inteligente podría desestabilizar la distribución de energía en una región, mientras que una vulnerabilidad en un dispositivo de monitorización médica podría poner en riesgo la salud o la vida del paciente. La falta de estándares de seguridad globales y la naturaleza fragmentada del ecosistema de IoT dificultan la implementación de soluciones de seguridad eficaces.

La privacidad es otro reto importante. Con la proliferación de dispositivos IoT se recopilan enormes cantidades de datos sobre las personas, desde sus hábitos de consumo hasta su ubicación y estado de salud. Estos datos, cuando se almacenan o comparten sin el consentimiento adecuado, pueden ser explotados por terceros, lo que plantea preocupaciones éticas y legales. Los usuarios a menudo no son conscientes del tipo de datos que sus dispositivos IoT están recopilando ni de cómo se utilizan o comparten esos datos.

Además, los dispositivos IoT generan grandes volúmenes de datos en tiempo real, lo que requiere infraestructuras robustas para almacenar, procesar y analizar esa información. Es decir, el IoT induce a una mayor adopción del Big Data para gestionar de manera eficiente estos datos, identificar patrones relevantes y tomar decisiones informadas. Sin embargo, a medida que crece el



volumen de datos, también aumenta la complejidad de su manejo, lo que puede generar problemas en términos de almacenamiento, procesamiento y privacidad.

Para abordar estos desafíos, es fundamental que las empresas y desarrolladores del IoT adopten mejores prácticas de seguridad y privacidad desde el diseño de los dispositivos y las redes. Esto incluye la implementación de encriptación de datos, la autenticación de dispositivos, la actualización continua del software para corregir vulnerabilidades, y la creación de marcos legales y regulatorios que protejan a los consumidores y usuarios.

## AUTOMATIZACIÓN E INTELIGENCIA ARTIFICIAL

Dos de los grandes pilares de la sociedad del dato son la automatización y la IA. La automatización de procesos se refiere a la utilización de tecnologías para realizar autónomamente tareas que tradicionalmente requerían de intervención humana. Este fenómeno ha existido durante décadas, pero ha alcanzado un nuevo nivel con los avances en robótica, software avanzado y sistemas de IA, lo que ha permitido automatizar procesos complejos y repetitivos en prácticamente todos los sectores. Desde líneas de producción en fábricas hasta servicios financieros y de atención al cliente, la automatización está transformando la forma en que las empresas operan, mejorando la eficiencia, reduciendo costes, acelerando la producción y aumentando la calidad y estabilidad de los procesos.

Como contrapartida, el impacto de la automatización en el empleo ha sido un tema de amplio debate. Por un lado, la automatización elimina la necesidad de muchos trabajos manuales y rutinarios, lo que ha provocado la reducción de empleos en ciertas áreas, como la industrial. Sin embargo, también genera nuevas oportunidades laborales en áreas como la programación, el análisis de datos y la ingeniería. En particular, la automatización ha fomentado el crecimiento de sectores tecnológicos y ha creado una demanda creciente de trabajadores con habilidades especializadas.

Uno de los efectos más notables de la automatización es el desplazamiento de ciertos tipos de empleo. Trabajos repetitivos y basados en reglas, como el ensamblaje de productos o la introducción de datos, han sido algunos de los primeros en ser automatizados. Este fenómeno ha llevado a la reconfiguración del mercado laboral, donde la demanda de habilidades técnicas, como el manejo de sistemas automatizados o el desarrollo de software, ha aumentado considerablemente. Sin embargo, el desafío radica en que no todos los trabajadores tienen las oportunidades o el acceso a la capacitación necesaria para adaptarse a este cambio, lo que contribuye a la polarización del mercado laboral, con empleos bien remunerados para trabajadores altamente cualificados y una disminución en las oportunidades para aquellos con menos formación.

A nivel macroeconómico, la automatización ha contribuido a un incremento significativo en la productividad. Las empresas que han adoptado tecnologías automatizadas han podido reducir tiempos de producción, minimizar errores y optimizar el uso de recursos. Esto ha generado un aumento en la competitividad y en la capacidad de innovación en diversos sectores. En sectores como la logística, por ejemplo, el uso de robots para el manejo de inventarios y la optimización de rutas de entrega ha transformado los modelos tradicionales de operación. En la agricultura, las máquinas automatizadas y los drones permiten a los agricultores optimizar las cosechas y utilizar los recursos de manera más eficiente.

Sin embargo, este incremento de la productividad o crecimiento económico a nivel macroeconómico no siempre se traduce en una distribución equitativa de los beneficios, lo que está llevando a un aumento de las desigualdades en algunas economías. Además, el temor al desplazamiento laboral genera preocupaciones sobre la estabilidad del empleo a largo plazo, lo que está impulsando debates sobre la necesidad de políticas que promuevan la capacitación continua y la reconversión de la fuerza laboral para adaptarse a las nuevas realidades del mercado.

## INTELIGENCIA ARTIFICIAL EN LA TOMA DE DECISIONES BASADA EN DATOS

En el ámbito de la automatización, la IA se ha convertido en una tecnología crucial, especialmente por su capacidad para tomar decisiones basada en datos, que permite a las máquinas y sistemas analizar grandes volúmenes de información y extraer conclusiones valiosas de manera rápida y eficaz. La IA utiliza técnicas avanzadas como el aprendizaje automático (*machine learning*) y el aprendizaje profundo (*deep learning*) para identificar patrones, hacer predicciones y proporcionar recomendaciones basadas en datos históricos y en tiempo real, lo que ayuda a automatizar tareas mucho más complejas, que requieran de cierto razonamiento para completarlas.

Uno de los principales beneficios de la IA es su capacidad para procesar y analizar grandes cantidades de datos mucho más rápido que cualquier ser humano. Esto es especialmente valioso en sectores como las finanzas, donde los algoritmos de IA pueden analizar mercados financieros y detectar oportunidades de inversión o riesgos en milisegundos. Asimismo, la IA se utiliza para mejorar operaciones empresariales, como la gestión de inventarios, el control de calidad en líneas de producción y la identificación de ineficiencias en las cadenas de suministro, proponiendo ajustes estratégicos u operativos de forma completamente automatizada.

En el ámbito de la salud, la IA está transformando la toma de decisiones vinculadas a un diagnóstico clínico. Los sistemas basados en IA pueden analizar imágenes médicas, como radiografías o resonancias magnéticas, y detectar anomalías con gran precisión, gracias a que estos sistemas son entrenados con muchos más datos y casos que los que cualquier especialista pueda llegar a conocer y estudiar en toda su vida. Así, ayudan a los médicos a diagnosticar enfermedades de manera más rápida y precisa. La IA también se utiliza en el desarrollo de tratamientos personalizados, en los que el análisis de datos genéticos y clínicos permite adaptar los tratamientos a las características individuales de cada paciente.

En el sector público, los gobiernos están utilizando la IA para mejorar la eficiencia en la prestación de servicios. Por ejemplo, se están implementando sistemas de IA para analizar datos poblacionales y predecir necesidades en áreas como la educación, la salud o la seguridad pública. Además, las soluciones de IA están siendo utilizadas para combatir el fraude en la administración pública, analizando patrones de comportamiento en transacciones financieras o en la declaración de impuestos.

A pesar de sus muchos beneficios, la utilización de la IA para automatizar tareas también plantea cuestiones éticas y de seguridad. Uno de los principales riesgos es el sesgo algorítmico, que puede surgir cuando los datos utilizados para entrenar los modelos de IA no son representativos o contienen prejuicios. Esto puede llevar a decisiones injustas o discriminatorias, especialmente en áreas sensibles como la concesión de créditos, la contratación de personal o la impartición de justicia.

Otro reto relacionado con la IA es la opacidad de los algoritmos. En muchos casos, los modelos de IA, especialmente aquellos basados en aprendizaje profundo, son "cajas negras" que proporcionan resultados sin una explicación clara de cómo llegaron a esas conclusiones. Esto plantea problemas de responsabilidad, pues es difícil para los usuarios y las instituciones comprender las bases de las decisiones tomadas por los sistemas de IA y, por consiguiente, dirigir una reclamación al culpable de una infracción o daño. Como resultado, se están desarrollando marcos regulatorios que promuevan la explicabilidad y la auditoría de los algoritmos de IA para garantizar que las decisiones sean comprensibles y justificables, aunque esto va en contra del propio desarrollo tecnológico de los sistemas, que funcionan como un todo, sin seguir la lógica tradicional.

Finalmente, la implementación generalizada de la IA plantea preguntas sobre el futuro del trabajo y el rol de las personas en la sociedad. A medida que la IA asume un papel más prominente en tareas que anteriormente requerían intervención humana, como el diagnóstico médico o la gestión



de inversiones, surge la preocupación de que las personas puedan volverse dependientes de los sistemas automatizados de IA, delegando cada vez más responsabilidades en las máquinas.

## "DATA SCIENCE", LA NUEVA RAMA DEL CONOCIMIENTO

La ciencia de datos ("*data science*", en inglés) es un campo interdisciplinar que combina conocimientos en estadística, matemáticas, programación y análisis de datos para extraer información útil a partir de grandes volúmenes de datos. En la era del Big Data, la ciencia de datos se ha convertido en una disciplina esencial para las organizaciones que buscan aprovechar al máximo sus datos y mejorar su toma de decisiones. Los científicos de datos son profesionales capacitados para recopilar, organizar, analizar e interpretar datos, y su demanda ha crecido exponencialmente en las últimas décadas debido a la creciente digitalización de todos los aspectos de la sociedad y la economía.

Uno de los factores que han impulsado la creciente demanda de científicos de datos es el volumen masivo de datos que se genera diariamente, que deben ser procesados utilizando las técnicas de Big Data ya mencionadas. Los datos generados a través de transacciones online, redes sociales, dispositivos móviles, sensores y otros medios deben ser transformados en conocimiento práctico para resultar de utilidad, lo que requiere de habilidades específicas que integran las disciplinas vinculadas a la ciencia de datos.

Entre estas habilidades destacan la programación en lenguajes como Python o R, la capacidad para manejar bases de datos complejas mediante SQL y el uso de herramientas de análisis y visualización de datos como Tableau o Power BI. Además, los científicos de datos deben tener un sólido conocimiento en estadística y modelado predictivo, ya que muchos de los enfoques utilizados en la ciencia de datos están diseñados para identificar patrones y realizar predicciones basadas en series históricas.

La creciente adopción de tecnologías basadas en datos ha llevado al surgimiento de nuevas profesiones y roles dentro de las empresas. Así, aparte de la denominación genérica "científico de datos", se encuentran categorías profesionales más o menos estándares en el mercado, como las siguientes:

- **Ingenieros de datos:** son los responsables de crear y mantener la infraestructura tecnológica que soporta el análisis de grandes volúmenes de datos.
- **Arquitectos de datos y especialistas en machine learning:** desarrollan modelos y algoritmos avanzados que permiten a las máquinas aprender de los datos y tomar decisiones autónomas.
- **Analistas de datos:** se encargan de interpretar los datos y presentar las conclusiones a los interesados de una forma comprensible.

La ciencia de datos no solo requiere habilidades técnicas, sino también de capacidad para comprender el contexto empresarial o social en el que se aplican los datos. Así, los científicos de datos deben estar cualificados para colaborar estrechamente con los equipos de marketing, finanzas, operaciones y otros departamentos para asegurarse de que los conocimientos extraídos de los datos tienen un impacto positivo directo y práctico.

## GOBERNANZA DE LOS DATOS

La gobernanza de los datos se refiere al conjunto de políticas, procesos y normativa que regulan cómo se recopilan, gestionan, almacenan, procesan y comparten los datos dentro de una organización o a escala internacional. Dado el creciente valor de los datos en la economía digital y el

papel fundamental que juegan en la sociedad, la correcta gestión de los datos es crucial para garantizar su uso ético, seguro y eficaz. Así, la gobernanza de los datos juega un papel crucial en la sociedad del dato. Los diferentes gobiernos y organismos supranacionales están estableciendo regulaciones para garantizar que el uso de los datos respete los derechos de los individuos y promueva la transparencia y la responsabilidad en las organizaciones que los manejan.

A medida que la economía digital ha ido creciendo, los países y regiones han ido desarrollando regulaciones específicas para proteger los datos personales y garantizar que las organizaciones actúan con ética y responsabilidad. Sin embargo, debido a la naturaleza global de las transacciones en el entorno online y las redes y repositorios de datos, las normativas nacionales deben alinearse con los estándares internacionales para garantizar que los datos puedan fluir libremente sin poner en riesgo la privacidad de los usuarios ni la seguridad de la información, mientras se permite la operación de las empresas que los gestionan. Algunas de las principales regulaciones internacionales son las siguientes:

- El Reglamento General de Protección de Datos (GDPR), aprobado por la UE en 2018, que establece un estándar global para la protección de la privacidad y la gestión de los datos personales.
- La Ley de Privacidad del Consumidor de California (CCPA), en EE. UU., que ofrece a los consumidores un mayor control sobre cómo se utilizan sus datos y les permite optar por no compartir su información con terceros.
- La Ley de Protección de Datos Personales (LGPD) de Brasil, que establece criterios para el tratamiento de datos personales y se considera un marco legal avanzado en Hispanoamérica.

Estas normativas tienen como objetivo principal asegurar que las organizaciones que recopilan y procesan datos lo hagan de manera ética y conforme a principios fundamentales como el consentimiento explícito, la transparencia y el derecho al olvido. En términos generales, las regulaciones internacionales establecen obligaciones para que las empresas gestionen los datos de manera adecuada, garantizando la seguridad y el cumplimiento normativo.

## PROTECCIÓN DE DATOS PERSONALES: EL ROL DEL GDPR Y OTRAS NORMATIVAS

El GDPR ha sido probablemente el desarrollo más importante en el ámbito de la protección de datos en todo el mundo. Su enfoque se centra en garantizar que las empresas e instituciones manejen los datos personales de los ciudadanos europeos de manera responsable y ética. Entre sus principios más importantes se encuentran:

- **Consentimiento explícito:** Las organizaciones deben obtener el consentimiento claro y explícito de los usuarios antes de recopilar y procesar sus datos. Esto asegura que los individuos tienen un control real sobre qué información están dispuestos a compartir y cómo se utilizará.
- **Derecho al olvido:** Los ciudadanos tienen el derecho a solicitar que sus datos personales sean eliminados cuando ya no sean necesarios para los fines para los que fueron recopilados o cuando retiren su consentimiento. Este principio brinda a los usuarios mayor control sobre su privacidad en la era digital.
- **Transparencia en el procesamiento de datos:** Las organizaciones deben informar de manera clara y transparente sobre cómo se recopilan, procesan y almacenan los datos, así como sobre los derechos de los usuarios en relación con sus datos. Esto incluye la obligación de notificar cualquier violación de seguridad que comprometa los datos personales.

El GDPR se ha convertido en un estándar global de facto, seguido en otras jurisdicciones para desarrollar sus normativas de protección de datos. En EE. UU., la CCPA de California ofrece

protecciones similares al GDPR, aunque con algunas diferencias, como otorgar a los consumidores el derecho de conocer a quién se venden sus datos personales. Por su parte, la LGPD de Brasil ha establecido criterios muy similares al GDPR para la recopilación y procesamiento de datos personales y ha sentado las bases para otros países hispanoamericanos.

Por último, conviene destacar que estas normativas, aunque son fundamentales en la economía digital, ya que los datos personales se han convertido en un activo valioso para las empresas que buscan personalizar sus productos y servicios, suponen frecuentemente un reto para las pymes, que deben cumplir con regulaciones complejas y, en algunos casos, costosas en términos de implementación.

## **TRANSPARENCIA Y RESPONSABILIDAD EN EL USO DE GRANDES VOLÚMENES DE DATOS**

A medida que el volumen de datos crece exponencialmente, las organizaciones se enfrentan a la creciente tarea de manejar estos datos de manera transparente y con un alto nivel de responsabilidad. La transparencia implica no solo comunicar claramente a los usuarios qué datos se recopilan y cómo se utilizan, sino también garantizar que estos datos se procesen de manera justa y de acuerdo con los principios éticos y legales establecidos, cuestión especialmente relevante cuando se utiliza la IA.

La responsabilidad en el manejo de grandes volúmenes de datos también implica implementar medidas de seguridad adecuadas para proteger la información de los usuarios frente a violaciones de datos o ataques cibernéticos. Las organizaciones deben asegurarse de que sus sistemas sean robustos y que cuenten con tecnologías como el cifrado de datos, la autenticación multifactor y la vigilancia continua de posibles amenazas. La falta de medidas de seguridad adecuadas no solo pone en riesgo a los usuarios, sino que también puede acarrear multas e implicaciones legales importantes bajo normativas como el GDPR.

También, como se ha indicado, la transparencia y la responsabilidad son esenciales en el uso de modelos y sistemas de IA que procesan grandes volúmenes de datos. Existe un riesgo significativo de que los sistemas algorítmicos introduzcan sesgos o discriminen a ciertos grupos de personas si no se diseñan y supervisan adecuadamente. Por esta razón, es fundamental que las organizaciones implementen procesos de auditoría y revisión que permitan garantizar que los modelos funcionen de manera justa y no trasladen prejuicios o desigualdades existentes en los datos ni creen otros nuevos. La explicabilidad de los algoritmos, es decir, la capacidad para comprender cómo se toman las decisiones automatizadas basadas en datos, se ha convertido en un tema de gran interés dentro del campo de la gobernanza de datos y se encuentra aún por resolver.

Finalmente, el concepto de responsabilidad corporativa se ha vuelto central en la gobernanza de datos. Las organizaciones deben ser responsables no solo ante los reguladores, sino también ante los usuarios y la sociedad en general. Esto incluye adoptar un enfoque proactivo para la gestión de datos, manteniendo un equilibrio entre el uso de los datos para mejorar productos y servicios y la protección de los derechos de los individuos.

## **LA ECONOMÍA DEL DATO**

Como ya se ha indicado, en la era digital, los datos se han convertido en uno de los recursos más valiosos de la economía global, a menudo referidos como el "nuevo petróleo", por su capacidad para impulsar la innovación y el crecimiento en una amplia gama de sectores, siempre que primero sean tratados adecuadamente ("refinados") para convertirlos en información útil. Los datos ofrecen una visión única sobre el comportamiento de los consumidores, las tendencias del mercado y la

eficiencia operativa y se han convertido en el pilar sobre el que se construyen los productos, servicios y estrategias empresariales en la actualidad.

El valor económico de los datos radica en su capacidad para generar conocimiento y ventajas competitivas. A diferencia de los recursos físicos, como el petróleo o el oro, los datos no se agotan con su uso; por el contrario, pueden ser reutilizados, combinados con otros conjuntos de datos y analizados de diferentes maneras para extraer nuevas ideas y oportunidades. Esta característica hace que los datos tengan un valor exponencial para las empresas que son capaces de aprovecharlos eficazmente. Cuantos más datos recopile una organización, más precisas serán sus predicciones y análisis, lo que le permitirá tomar decisiones mejor fundamentadas y mejorar sus procesos.

Además, los datos son fundamentales para la personalización de productos y servicios, un aspecto clave en la economía digital. Empresas como Amazon, Netflix y Google utilizan los datos de sus usuarios para ofrecer recomendaciones personalizadas, lo que no solo mejora la experiencia del cliente, sino que también incrementa el valor percibido de sus servicios, aumentando así la lealtad y el nivel de gasto en ellos por parte de los usuarios. La capacidad de recopilar y analizar datos en tiempo real permite a las organizaciones responder rápidamente a los cambios en la demanda del mercado, optimizando su oferta y anticipando las necesidades de los consumidores.

En términos macroeconómicos, el valor económico de los datos también está ligado a su potencial para impulsar la eficiencia en las cadenas de suministro, mejorar la toma de decisiones en políticas públicas, y fomentar la innovación en áreas como la salud, la educación y la energía. Los datos permiten una mejor planificación, seguimiento y evaluación de programas y proyectos, lo que a su vez impulsa un crecimiento más sostenible y equitativo.

## MODELOS DE NEGOCIO BASADOS EN DATOS

Este valor de los datos ha producido un fenómeno ciertamente curioso en la última década: la proliferación de modelos de negocio basados en datos, impulsados por la capacidad de las empresas para recolectar, procesar y analizar grandes volúmenes de datos. Estos modelos son actualmente esenciales en la economía digital y se encuentran en el núcleo de muchas de las empresas más exitosas del mundo.

Uno de los modelos más destacados es el de las plataformas digitales, que actúan como intermediarios entre usuarios y proveedores de servicios. Ejemplos como Uber, AirBnB, Wallapop y Amazon no solo operan como plataformas de servicios, sino que también monetizan los datos que recopilan de sus usuarios a través de publicidad dirigida y ventas de productos y servicios, que muchas veces ni siquiera poseen ni prestan. En este tipo de modelo, los datos de los usuarios se utilizan para segmentar audiencias, personalizar ofertas y mejorar la eficacia de las campañas publicitarias, lo que genera ingresos sustanciales. En otros casos, como las redes sociales o el buscador de Google, los datos de comportamiento de los usuarios (como búsquedas, compras y preferencias de navegación) son el principal recurso que alimenta este ecosistema para generar ingresos por publicidad.

Otro modelo de negocio basado en datos es el de los servicios de análisis y consultoría. Muchas empresas no tienen la infraestructura o las habilidades para aprovechar plenamente sus propios datos, por lo que recurren a terceros que ofrecen soluciones de analítica de datos. Empresas como IBM, Accenture y SAS proporcionan servicios de análisis de Big Data que ayudan a otras organizaciones a tomar decisiones estratégicas basadas en información cuantitativa. Estos modelos de negocio son lucrativos porque permiten a las organizaciones transformar grandes cantidades de datos en conocimiento útil, mejorando así su competitividad y eficiencia.

El modelo de productos como servicio (*Product-as-a-Service*) también está impulsado por los datos. En lugar de vender productos físicos, las empresas recopilan datos sobre el uso de sus productos

para ofrecer servicios de valor añadido. Un ejemplo de esto es el modelo de renting de coches personalizado, donde las empresas recopilan datos sobre cómo los clientes utilizan los vehículos y utilizan esta información para mejorar continuamente la oferta y personalizar la experiencia del usuario. Además, en industrias como la manufactura, los datos de los sensores de los equipos permiten a las empresas ofrecer servicios de mantenimiento predictivo, donde pueden anticipar problemas antes de que ocurran y realizar reparaciones preventivas.

Finalmente, el comercio electrónico es otro sector impulsado por modelos basados en datos. Las plataformas de venta online recopilan y analizan datos sobre las preferencias y hábitos de compra de los consumidores, lo que les permite optimizar su inventario, personalizar la experiencia de compra y recomendar productos que sean relevantes para cada usuario. Esto aumenta las tasas de conversión y mejora la satisfacción del cliente, creando una relación más sólida entre la empresa y el consumidor, sin necesidad de una tienda física y, en ocasiones, ni siquiera almacén de productos, ya que son adquiridos directamente del fabricante conforme el cliente final los compra (el denominado "dropshipping").

## MONOPOLIOS DIGITALES Y CONCENTRACIÓN DE PODER

Uno de los efectos secundarios del crecimiento de la economía del dato está siendo la concentración de poder en manos de un pequeño número de empresas tecnológicas, conocidas como gigantes tecnológicos o "Big Tech". Empresas como Google, Facebook, Amazon, Apple y Microsoft dominan gran parte del ecosistema digital y controlan enormes cantidades de datos sobre los usuarios, lo que les otorga una ventaja competitiva desproporcionada frente a otras compañías más pequeñas o tradicionales e, incluso, un poder desmesurado ante gobiernos y países.

El control de los datos es uno de los principales factores que contribuyen a la formación de monopolios digitales. Cuantas más interacciones y transacciones puedan registrar y analizar estas empresas, más preciso será su conocimiento sobre los usuarios y el mercado en general. Esto les permite mejorar sus servicios de manera constante y atraer a más usuarios, creando un efecto red que dificulta la competencia. Por ejemplo, Google utiliza su dominio en el ámbito de las búsquedas online y la publicidad digital para generar ingresos que luego reinvierte en la adquisición de otras empresas y en la mejora de sus productos, consolidando aún más su posición. Facebook (ahora Meta) aprovechó sus enormes recursos económicos para adquirir Instagram y después WhatsApp, convirtiéndose prácticamente en el proveedor único de redes sociales generalistas en Occidente, con la excepción de X.

La concentración de datos también ha llevado a preocupaciones sobre la falta de competencia y los posibles abusos de poder. Las grandes empresas tecnológicas controlan no solo el acceso a los datos, sino también las plataformas a través de las cuales se accede a ellos. Esto ha dado lugar a críticas por parte de reguladores y gobiernos, que argumentan que estas empresas han acumulado un poder excesivo, que les permite anular la competencia, controlar los precios y limitar la innovación en ciertos sectores. En respuesta, ha habido algunos llamamientos para regular más estrictamente a las Big Tech y fomentar una mayor competencia en el espacio digital, aunque ciertamente con muy poco éxito.

Otro aspecto problemático de los monopolios digitales es su capacidad para influir en la privacidad de los usuarios. Al controlar grandes volúmenes de datos personales, estas empresas tienen acceso a información detallada sobre los hábitos, intereses y comportamientos de millones de personas. Si bien los usuarios consienten compartir sus datos a cambio de servicios gratuitos o personalizados con bastante frecuencia, la enorme cantidad de datos disponibles, combinada con el uso de la IA, permite extraer muchos más datos sobre los usuarios, aunque estos no hayan sido legalmente cedidos (lo que se conoce técnicamente como "aumento de datos" ("*data augmentation*", en

inglés). Además, el uso que las empresas hacen de estos datos no siempre es transparente. Las violaciones de privacidad y el uso indebido de los datos, como se vio en el escándalo de Cambridge Analytica y otros muchos en época reciente, han generado un mayor escrutinio sobre cómo las grandes plataformas tecnológicas manejan la información de los usuarios.

Finalmente, la concentración de poder en el ámbito de los datos también tiene implicaciones para la seguridad y soberanía digital. Al depender de un pequeño número de proveedores de servicios tecnológicos, tanto empresas como gobiernos corren el riesgo de quedar expuestos a posibles fallos o vulnerabilidades de seguridad en estas plataformas, como ocurrió recientemente con la caída del servicio Azure de Microsoft, que dejó sin servicio a muchas empresas y servicios gubernamentales, incluidas aerolíneas y bancos. Además, la dependencia de infraestructuras tecnológicas controladas por empresas extranjeras plantea cuestiones serias sobre la soberanía digital y el control que los países tienen sobre los datos de sus ciudadanos.

## **LA SOCIEDAD DEL DATO**

En este artículo se acuña el concepto "sociedad del dato" por primera vez para describir el siguiente estado de madurez tecnológica de la sociedad, en la que nos encontramos. La sociedad del dato se diferencia de la sociedad de la información en que la abundancia de datos en los entornos digitales comienza a presentar amenazas y problemas serios para la propia sociedad. Así, mientras en la sociedad de la información los datos son una herramienta útil para mejorar procesos e interacciones entre las personas y las organizaciones, en la sociedad del dato, la superproducción de datos a gran velocidad, gran parte de ellos con dudosa o nula utilidad, representa un problema que afecta no solo al consumo de recursos naturales (energía, tierras raras, etc.) que pueden representar un problema medioambiental, sino también al propio funcionamiento de la sociedad, dificultando las relaciones humanas en cuanto a confianza, comunicación e, incluso, la libertad del individuo y su capacidad cognitiva.

A continuación, se describen los principales factores y características que definen la sociedad del dato y sus posibles consecuencias futuras.

## **DATOS MASIVOS Y VOLÁTILES**

La sociedad del dato se caracteriza por la producción, almacenamiento y análisis de cantidades masivas de información en tiempo real. Esta explosión de datos, conocida como Big Data, es impulsada por el crecimiento de dispositivos conectados, la digitalización de la vida diaria y la capacidad de las organizaciones para recopilar datos de múltiples fuentes. Esta explosión digital fue ampliamente apoyada por las medidas adoptadas durante la pasada pandemia de COVID-19, donde tanto organizaciones privadas como organismos públicos en todo el mundo adoptaron medidas para realizar todos los trámites e interacciones posibles de forma online, evitando el desplazamiento y contacto físico entre las personas.

Una vez alcanzado el elevado nivel de digitalización actual, uno de los retos principales a los que se enfrenta la sociedad del dato es la volatilidad de los datos. Resulta evidente que, en la actualidad, se generan datos de manera continuada y en cantidades sin precedentes, pero su valor puede ser temporal o efímero. La rapidez con la que la información se vuelve obsoleta obliga a las organizaciones a procesar y actuar sobre los datos en tiempo real para aprovechar al máximo su potencial antes de que pierdan relevancia, además de a decidir qué datos deben ser descartados o si, por el contrario, se deciden conservar todos los datos, lo que a largo plazo puede resultar insostenible.



Así, la naturaleza masiva de los datos en la actualidad plantea problemas para su gestión, análisis y toma de decisiones. Mientras que los datos pueden proporcionar información valiosa, el volumen y la velocidad a la que se generan pueden hacer que las organizaciones se vean abrumadas, perdiendo la capacidad de distinguir entre información relevante e irrelevante.

## **DATOS IRRELEVANTES Y BASURA DIGITAL**

Un fenómeno emergente en la sociedad del dato es la acumulación de datos irrelevantes o inútiles, también conocida como basura digital. A medida que las organizaciones y los individuos recopilan cada vez más datos, una gran parte de estos carece de valor o relevancia. Este tipo de datos no solo ocupan espacio de almacenamiento, sino que también pueden dificultar la capacidad de encontrar información valiosa o tomar decisiones informadas. La sobreabundancia de datos sin procesar puede actuar como una barrera para la innovación y la eficiencia, ya que las organizaciones deben filtrar grandes cantidades de información inútil antes de llegar a los datos que realmente importan.

Este problema se agrava en el ámbito de las redes sociales y plataformas de contenido, donde las publicaciones, comentarios y contenido generado por usuarios inunda las plataformas sin una validación clara de su relevancia o veracidad. La basura digital no solo es una carga para la infraestructura tecnológica, sino que también afecta la calidad de la información disponible para los usuarios. En la actualidad, no existe conciencia alguna por parte de los usuarios de que, cada vez que están publicando un mensaje, imagen o vídeo en una red social, están sobrecargando el ecosistema de centros de datos que soporta la infraestructura de esa red, provocando un daño al medioambiente, entre otras cuestiones.

Además, la facilidad con la que cualquiera puede hacer publicaciones en casi cualquier medio hace que, por pura estadística, gran parte de los contenidos existentes en Internet sean irrelevantes, imprecisos e incluso totalmente erróneos, sin que se haya concebido aún una manera de discernir qué contenidos proceden de fuentes más o menos cualificadas y cuáles no. Esto representa un serio problema a la preservación del conocimiento pues, si disminuye el reconocimiento a las fuentes primarias en papel u otros soportes físicos en pro del uso de información digital, el riesgo de perder gran parte del conocimiento legado por nuestros antepasados, mezclado y perdido entre la basura digital, podría dar lugar a una nueva era de oscuridad similar a lo que supuso la Edad Media para el legado clásico.

## **SISTEMAS DE PUNTUACIONES Y RECOMENDACIONES**

Un factor que suma más riesgo a la preservación y búsqueda del conocimiento en la sociedad del dato son los sistemas de puntuaciones y recomendaciones. En la sociedad del dato, estos sistemas juegan un papel fundamental en la forma en que interactuamos con productos, servicios y personas. Estos sistemas, impulsados por algoritmos de IA, evalúan a los usuarios, productos o contenidos basados en datos recopilados previamente para ofrecer recomendaciones personalizadas. Plataformas como Amazon, Netflix y Spotify utilizan estos sistemas para sugerir productos, series o música en función del comportamiento de los usuarios, lo que ha mejorado significativamente la experiencia del consumidor.

Sin embargo, aunque estos sistemas pueden ser altamente beneficiosos para detectar macrotenencias o categorizar a productos y personas en determinados tipos de patrones de comportamiento, siempre se basan en la afirmación de que el promedio de un número elevado de mediciones suele ofrecer el valor más probable o preciso de una variable (lo que se conoce como confianza en estadística). Sin embargo, esto tiene varios inconvenientes:

- En **conjuntos de muestras reducidos**, el nivel de confianza es muy bajo. Por ejemplo, si un libro tiene solo dos reseñas, el promedio de puntuación de esos usuarios no tiene confianza alguna. Sin embargo, todos los motores de búsqueda actuales ofrecen el número de “estrellas” mezclado, sin ponderar o filtrar aquellos promedios con muy pocas muestras. Esto ofrece una realidad distorsionada, que muchas veces se tiene en cuenta para tomar decisiones erróneas.
- La **cualificación de las muestras** puede ser muy diferente y, sin embargo, nunca se pondera. En el mismo ejemplo anterior, la reseña de un miembro de la Real Academia de la Lengua Española o de un fiel seguidor del autor del libro tiene el mismo peso que la que ha realizado un analfabeto que simplemente hizo clic en una puntuación sin ser ni siquiera consciente de tal acto.
- El **envenenamiento de los datos**, es decir, introducir muestras falsas con una intención perversa, está generalmente poco o nada controlado en la mayoría de estos sistemas, existiendo directamente muchas reseñas falsas o generadas por “bots” (robots de software que realizan tareas automáticamente sobre aplicaciones y servicios digitales).

La consecuencia de la proliferación y adopción ciega de estos sistemas de puntuaciones y recomendaciones abiertos a la comunidad es que, cada vez más, se toman decisiones de mayor calado basadas en análisis y conclusiones de datos de escasa o nula representatividad, conduciéndonos a una sociedad enfocada en “dirigir” tales reseñas y puntuaciones, en vez de estarlo en resolver los problemas reales. Haciendo una analogía con la conducción de un vehículo, si el conductor pone el foco en estudiar y modificar la posición del volante en vez de observar y analizar hacia dónde va el trazado de la carretera, el accidente está asegurado en poco tiempo.

## FAKES, MARGINACIÓN, CENSURA DIGITAL Y VERIFICADORES DE LA VERDAD

Otra cuestión importante es que, en la sociedad del dato, el acceso a la información no siempre garantiza la veracidad de los contenidos. La proliferación de *fake news* y desinformación ha erosionado la confianza en los medios digitales y ha complicado la tarea de identificar lo que es verdadero y lo que no lo es. Esta situación ha dado lugar a la creación de verificadores de la verdad, plataformas y organizaciones dedicadas a contrastar la información y desmentir noticias falsas.

Sin embargo, la censura digital y la marginación de ciertas voces en el mundo online son fenómenos que también preocupan en este contexto. Gobiernos y grandes plataformas tecnológicas tienen el poder de restringir o eliminar contenido, lo que puede ser utilizado como una herramienta de control político o social. En algunos casos, la censura puede justificar la eliminación de desinformación, pero en otros, puede silenciar a disidentes o minorías.

La frontera entre la protección de la verdad y la imposición de la censura es frecuentemente difusa, lo que plantea un reto en términos de libertad de expresión y acceso a información plural. Esto es un serio problema en la actualidad, donde las agencias verificadoras de la verdad (*fact checking*, en inglés) son gestionadas como cualquier otra empresa privada, con muy poca o ninguna regulación de los estados. Mientras en otros campos como la medicina, el sector energético, la banca o la educación existen regulaciones estrictas y requisitos muy concretos de transparencia y auditoría para las empresas que operan en estos sectores e, incluso, en actividades específicas, los verificadores de la verdad se mueven en un ámbito de cuasi-soberanía sobre la Verdad, es decir, que estas agencias podrían servir a otras organizaciones como su brazo censor y de propaganda, de manera muy similar a lo que se vivió durante los gobiernos socialistas nazis y de la URSS en la primera mitad del siglo XX en Europa.

Como consecuencia, se habla del concepto de “marginación digital”, referido a la exclusión de ciertas personas o comunidades del acceso a las plataformas y redes donde se distribuye la



información y puede deberse no solo a motivos económicos o geográficos como los que provoca la brecha digital, ya mencionada, sino también a cuestiones políticas o a intereses económicos de los poderes fácticos, lo que también podría dirigir la sociedad actual hacia el oscurantismo de una nueva Edad Media, cercenando derechos y libertades y, por ende, con los modelos democráticos desplegados durante el siglo pasado en muchos países.

## **EL DATO COMO RECURSO PARA OCULTAR INFORMACIÓN**

Resulta curioso, en la sociedad actual, que aunque los datos se consideran una fuente de transparencia e información, también pueden ser utilizados para ocultar información. Las organizaciones pueden presentar grandes volúmenes de datos de manera confusa o incompleta para disfrazar la realidad de una situación. Por ejemplo, el uso excesivo de cifras o estadísticas sin un contexto adecuado puede manipular la percepción del público sobre determinados hechos. De igual manera, inundar las redes sociales con mensajes sin contenido real o con la información contraria a la revelada por una fuente cualificada es una práctica bastante habitual para dificultar el acceso a tal fuente.

En algunos casos, los gobiernos o empresas pueden publicar datos que, a primera vista, parecen transparentes, pero que en realidad omiten información crítica o presentan datos de manera que distraen de los verdaderos problemas. Esta estrategia de "ocultar a plena vista" convierte al dato en un instrumento para confundir más que para aclarar, dificultando a los ciudadanos o analistas acceder a la información clave para tomar decisiones informadas.

## **EL DATO COMO HERRAMIENTA DE PROPAGANDA Y MANIPULACIÓN DE LA MASA**

Tal como se ha comentado, mediante las distintas técnicas comentadas y otras existentes, el dato puede ser utilizado como una herramienta para la propaganda y la manipulación de la masa. A través del análisis de datos, las empresas y gobiernos pueden identificar los intereses, preocupaciones y deseos de los individuos y utilizar esta información para crear mensajes persuasivos diseñados para influir en sus opiniones y comportamientos. Esta capacidad de personalizar la propaganda ha hecho que las campañas políticas, las campañas publicitarias y otros tipos de influencias masivas sean mucho más eficaces, sobre todo con el uso de la IA para analizar los datos de redes sociales y otros patrones de comportamiento de las personas.

Las plataformas digitales permiten a los actores interesados segmentar a los usuarios en grupos específicos y enviarles mensajes cuidadosamente elaborados para maximizar el impacto. Esta técnica, conocida como microtargeting, ha sido ya utilizada ampliamente en campañas políticas recientes y plantea preguntas sobre la manipulación de la opinión pública y la ética de utilizar datos personales para influir en decisiones democráticas. Sin embargo, parece que la sociedad del dato no solo acepta, sino que promueve este tipo de prácticas como sanas y deseables.

## **DATOS PARA EL FUTURO**

En la actualidad, el uso de datos para realizar análisis predictivos ha ganado gran importancia. La capacidad de prever futuros comportamientos y tendencias basándose en datos históricos está transformando áreas como el marketing, la medicina, la seguridad y la planificación urbana. Las tecnologías predictivas permiten a las empresas anticipar la demanda de productos, a los gobiernos prever el tráfico o el consumo energético, y a los médicos identificar posibles enfermedades antes de que estas se manifiesten.

Sin embargo, la dependencia de los datos para hacer predicciones también puede ser problemática. Las predicciones basadas en datos tienden a reforzar los patrones existentes y pueden perpetuar

desigualdades o sesgos, si estos se producen en el presente. El análisis de series históricas tampoco predice comportamientos acíclicos o sobrevenidos por eventos fortuitos. Sin embargo, las organizaciones, se encuentra actualmente obsesionadas con disponer de cuantos más datos mejor, especialmente actualmente, con el auge de los sistemas de IA, que requieren grandes conjuntos de muestras para ser entrenados.

Conviene recordar cómo los proveedores de las grandes redes sociales (Meta, LinkedIn, X, etc.) han ido guardando todo el historial de publicaciones e interacciones de sus usuarios desde el principio, incluso de cuentas que han sido aparentemente eliminadas por sus usuarios. Quizás con la visión de que, cuando los sistemas de IA fueran capaces de analizar estos enormes repositorios para extraer patrones e información sobre los usuarios, estos datos serían valiosos, se fueron almacenando todos ellos durante más de una década y ahora obtienen el rédito económico que este coste ha tenido para ellos en el pasado. Por el mismo motivo, en la actualidad se siguen almacenando ingentes cantidades de datos en los centros de datos, hasta el punto de que se cuestiona la sostenibilidad ya no solo ambiental sino energética para alimentar estos centros, con el interés de disponer de recursos para desarrollar los modernos sistemas de IA. Un ejemplo llamativo es el reciente acuerdo de Google con la empresa americana Kairos Power para fabricar pequeños reactores nucleares junto a sus centros de datos para disponer de la energía suficiente para alimentarlos.

## **EL SER HUMANO COMO ESCLAVO DIGITAL**

Para concluir, uno de los riesgos de la sociedad del dato es que el ser humano se convierta en un esclavo digital, atrapado en un ciclo de producción y consumo de datos. A medida que los individuos pasan más tiempo en Internet, consumiendo servicios digitales, generando datos a través de sus interacciones, transacciones y comportamientos, las empresas y gobiernos pueden utilizar esta información para influir en sus decisiones y controlar sus comportamientos. El concepto de "esclavitud digital" se refiere a la falta de autonomía que los individuos pueden experimentar en un mundo donde cada acción está monitorizada y registrada, y donde las decisiones se toman en función de los datos recopilados sobre ellos.

En este contexto, las personas pueden perder el control sobre su privacidad y su identidad, y encontrarse atrapadas en una infraestructura digital que las categoriza, segmenta y evalúa en función de los datos que producen. Dado el impacto que estas cuestiones representa sobre su vida, es probable que comience a prestar bastante más interés en su "vida digital" que en su universo físico y real. Esta situación plantea serias preocupaciones sobre el futuro de la libertad individual en una sociedad dominada por el dato y la tecnología. En este contexto, el movimiento transhumanista pretende desdibujar la frontera entre el mundo físico y digital del individuo, ya sea desarrollando interfaces entre ambos entornos (como el sistema que está desarrollando la empresa Neuralink, de Elon Musk, para conectar el cerebro humano a un ordenador) o fomentando el desarrollo de un entorno inmersivo interconectado (el Metaverso) que sustituya al real en un mayor número de actividades (viajes, entretenimiento, conciertos, reuniones de trabajo y sociales, etc.).

## **CIBERSEGURIDAD EN LA ERA DEL DATO**

Para concluir, es importante destacar que, en la era del dato, la ciberseguridad se ha convertido en una preocupación crítica para gobiernos, empresas y ciudadanos, ya que el volumen de datos generados, almacenados y procesados continúa creciendo exponencialmente, muchas veces fuera de control. La proliferación de dispositivos conectados a Internet, el aumento de las plataformas digitales y el uso masivo de servicios en la nube han dado lugar a un ecosistema donde las amenazas cibernéticas son más frecuentes y sofisticadas. Algunas de las principales amenazas a las que se enfrenta la sociedad del dato son:

- **Ciberataques:** Los ciberataques son intentos maliciosos de acceder a sistemas de información para robar, alterar o destruir datos. Los ataques pueden ser perpetrados por individuos, grupos organizados o incluso por actores estatales, y pueden tener como objetivo tanto entidades públicas como privadas. Los ataques de *ransomware*, donde los atacantes cifran los datos de una organización y exigen un rescate a cambio de su liberación, se han vuelto especialmente comunes y devastadores en los últimos años.
- **Filtraciones de datos:** Una de las vulnerabilidades más importantes en la sociedad del dato es el riesgo de filtraciones de información sensible. Esto puede ocurrir a través de hackeos, fallos de seguridad o errores humanos. Las filtraciones de datos pueden exponer información personal, como nombres, direcciones, números de tarjetas de crédito y datos de salud, lo que afecta tanto a individuos como a empresas y gobiernos.
- **Ataques a infraestructuras críticas:** En un mundo cada vez más digitalizado, las infraestructuras críticas (como la energía, el transporte, la sanidad o las telecomunicaciones) dependen en gran medida de los datos y los sistemas conectados. Esto las convierte en objetivos atractivos para los cibercriminales. Un ataque a una central eléctrica, por ejemplo, podría generar un apagón a gran escala, con consecuencias graves para la seguridad y el bienestar de la población.
- **Phishing y suplantación de identidad:** El phishing es una táctica común utilizada por los atacantes para engañar a las personas para que revelen información personal o credenciales de acceso, a menudo mediante correos electrónicos, llamadas telefónicas o SMS fraudulentos que parecen provenir de fuentes confiables. Una vez que los atacantes obtienen esta información, pueden acceder a sistemas críticos, robar identidades o cometer fraudes financieros.
- **Dispositivos IoT y vulnerabilidades en redes conectadas:** El auge del IoT ha incrementado significativamente el número de dispositivos conectados, desde termostatos inteligentes hasta vehículos autónomos. Sin embargo, como se ha visto, muchos de estos dispositivos no cuentan con medidas de seguridad robustas, lo que los convierte en puntos de entrada para los ciberataques. La interconectividad de estos dispositivos en redes masivas amplía la superficie de ataque, lo que pone en riesgo no solo a los usuarios individuales, sino también a las infraestructuras y organizaciones que dependen de estos sistemas.
- **Amenazas internas:** Las organizaciones también afrontan riesgos de amenazas que provienen de empleados actuales o antiguos que tienen acceso a datos sensibles. Estas personas pueden divulgar información de manera accidental o intencionada, lo que genera violaciones de seguridad y filtraciones de datos.

## MECANISMOS DE PROTECCIÓN Y REGULACIÓN EN CIBERSEGURIDAD

Para hacer frente a estas amenazas, se han desarrollado diversos mecanismos de protección y normativas que buscan garantizar la seguridad de los datos y la protección de la información. Estos mecanismos se implementan tanto a nivel organizacional como regulatorio, y son esenciales para mantener la integridad, confidencialidad y disponibilidad de los datos en un entorno cada vez más vulnerable.

- **Cifrado de datos:** El cifrado es una de las herramientas más efectivas para proteger la información sensible. Mediante el uso de algoritmos criptográficos, los datos se codifican de manera que solo puedan ser leídos por las partes autorizadas que posean las claves de descifrado. El cifrado se utiliza tanto en el almacenamiento de datos como en su transmisión a través de redes, lo que minimiza el riesgo de que la información sea interceptada o robada.
- **Autenticación multifactor (MFA):** La autenticación multifactor es una medida de seguridad que requiere que los usuarios proporcionen más de una forma de verificación antes de acceder a un sistema o servicio. Esto puede incluir una combinación de contraseñas, códigos

enviados por mensaje de texto, huellas dactilares o escaneo de retina. La MFA ayuda a prevenir accesos no autorizados, incluso si las contraseñas de los usuarios son comprometidas.

- **Monitorización de redes y detección de intrusiones:** La monitorización constante de las redes es crucial para detectar actividades sospechosas y prevenir ataques antes de que causen daños significativos. Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) son herramientas diseñadas para analizar el tráfico de la red y alertar a los administradores cuando se detectan comportamientos anómalos que podrían indicar un ciberataque en curso.
- **Normativas de ciberseguridad:** En el ámbito internacional se han promulgado distintas leyes para garantizar la seguridad de los datos y establecer obligaciones para las organizaciones que procesan información. El GDPR, además de proteger la privacidad, incluye disposiciones sobre la seguridad de la información, como la obligación de notificar a las autoridades en caso de violaciones de datos. Del mismo modo, la CCPA de California regula cómo las empresas deben proteger los datos personales de los consumidores.
- **Formación en ciberseguridad:** Las empresas y organizaciones deben invertir en la formación de su personal para que los empleados sean conscientes de las amenazas cibernéticas y puedan actuar como la primera línea de defensa. La formación en ciberseguridad incluye identificar correos de phishing, respetar buenas prácticas en la gestión de contraseñas y evitar el acceso a redes no seguras.
- **Firewalls y antivirus:** Los firewalls son barreras de seguridad que filtran el tráfico de entrada y salida de las redes para evitar que entes malintencionados accedan a los sistemas. Los antivirus, por su parte, son programas diseñados para detectar y eliminar software malicioso. Juntos, estos mecanismos protegen las redes y los dispositivos de ataques externos.

## EL FUTURO DE LA SEGURIDAD DE LA INFORMACIÓN

El futuro de la seguridad de la información está íntimamente ligado a los avances tecnológicos y a la creciente complejidad de las amenazas cibernéticas. A medida que los cibercriminales desarrollan nuevas tácticas y herramientas para evadir los mecanismos de defensa, las organizaciones deben estar preparadas para adaptarse e innovar en sus estrategias de seguridad.

- **Inteligencia artificial:** La IA jugará un papel fundamental en el futuro de la ciberseguridad. Estas tecnologías permiten a los sistemas identificar patrones de comportamiento y anomalías en el tráfico de red en tiempo real, lo que facilita la detección proactiva de amenazas y la respuesta automática a incidentes. Además, la IA puede ayudar a reducir la carga sobre los equipos de seguridad al automatizar tareas como el análisis de alertas y la identificación de vulnerabilidades.
- **Ciberseguridad en el IoT:** A medida que el IoT continúa expandiéndose, los dispositivos conectados se convertirán en uno de los principales focos de atención en términos de ciberseguridad. La seguridad de estos dispositivos será crucial para proteger infraestructuras críticas y evitar ciberataques a gran escala. En el futuro, se espera el desarrollo de estándares de seguridad más estrictos para los dispositivos IoT, así como la implementación de tecnologías de autenticación más robustas.
- **Ciberseguridad cuántica:** Con la llegada de la computación cuántica, los métodos actuales de cifrado podrían quedar obsoletos, ya que los ordenadores cuánticos tendrán la capacidad de romper muchos de los algoritmos criptográficos actuales de forma prácticamente instantánea. Esto ha llevado a la investigación en ciberseguridad cuántica, que busca desarrollar nuevas técnicas de cifrado que sean resistentes a los ataques de ordenadores cuánticos.

- **Cero confianza (Zero Trust):** El enfoque de "cero confianza" es un modelo emergente en ciberseguridad que asume que ninguna entidad dentro o fuera de una red puede ser completamente confiable. Este enfoque implica verificar constantemente la identidad de los usuarios y dispositivos que acceden a los sistemas y aplicar controles de seguridad rigurosos en cada punto de acceso, minimizando así el riesgo de ataques internos y externos.
- **Regulación y cooperación internacional:** Dado que las amenazas cibernéticas no conocen fronteras, el futuro de la ciberseguridad también dependerá de la cooperación internacional. Los gobiernos y las organizaciones globales deberán trabajar juntos para establecer estándares comunes y marcos de colaboración que faciliten el intercambio de información y mejores prácticas para combatir el cibercrimen. Organizaciones como la Interpol, la UE y el Foro Económico Mundial están impulsando iniciativas para mejorar la colaboración internacional en ciberseguridad, lo que permitirá una respuesta más coordinada y eficiente a los ataques que cruzan fronteras. Además, la creación de tratados internacionales sobre ciberseguridad podría establecer pautas claras sobre la cooperación entre naciones, la persecución de delitos cibernéticos y la protección de infraestructuras críticas.
- **Privacidad por diseño:** En el futuro, es probable que las empresas adopten un enfoque más proactivo hacia la privacidad y la seguridad, implementando principios de privacidad por diseño ("*privacy by design*", en inglés) en el desarrollo de sus productos y servicios. Esto significa que la seguridad de los datos y la privacidad del usuario se integrarán en la fase de diseño de los sistemas, en lugar de ser una adición posterior. Este enfoque garantizaría que las aplicaciones y servicios digitales cumplan con los estándares de seguridad desde el principio, minimizando los riesgos a vulnerabilidades.
- **Conciencia social y cultura de ciberseguridad:** A medida que las amenazas cibernéticas evolucionen, también será fundamental promover una mayor conciencia social sobre los riesgos asociados con el uso de tecnologías conectadas. Las campañas educativas para el público general sobre buenas prácticas en ciberseguridad, como la protección de contraseñas, el reconocimiento de intentos de phishing y la importancia de la privacidad digital, serán cruciales para fortalecer la primera línea de defensa ante ciberataques. Fomentar una cultura de ciberseguridad en todos los niveles, desde los usuarios hasta las grandes corporaciones, es esencial para garantizar que todos los actores estén alineados en la protección de la información.

## CONCLUSIONES

Este artículo acuña el concepto de "sociedad del dato" como una nueva etapa en la historia reciente de la humanidad, que representa un cambio profundo en la manera en que los individuos, las organizaciones y los gobiernos recopilan, procesan y utilizan la información. A diferencia de etapas anteriores, como la sociedad de la información y del conocimiento, donde la información era principalmente un medio para la comunicación y la toma de decisiones informadas, en la actualidad, el volumen masivo de datos generados y la capacidad tecnológica para analizar y manipular dicha información, especialmente apoyada por la IA, han dado lugar a una sociedad en la que los datos son un recurso esencial, el centro de las interacciones sociales, con un impacto global en múltiples aspectos de la vida cotidiana, la economía y la política.

Este nuevo paradigma presenta oportunidades importantes. La posibilidad de analizar grandes cantidades de datos en tiempo real permite avances en áreas como la medicina, donde el diagnóstico y tratamiento personalizados se vuelven cada vez más precisos, o en la optimización de procesos industriales, que incrementan la eficiencia y reducen costos. Además, los datos abren la puerta a modelos de negocio innovadores y a la personalización de servicios, lo que en última instancia mejora la experiencia del usuario.

Sin embargo, la sociedad del dato plantea retos y riesgos importantes. La sobreabundancia de datos irrelevantes, la creciente basura digital y la posibilidad de manipulación de la información a través de sistemas de recomendación y sistemas de IA crean un entorno donde distinguir la verdad de la desinformación es cada vez más difícil. Además, la concentración de poder en manos de grandes empresas tecnológicas ha dado lugar a monopolios digitales que dominan el acceso a los datos y limitan la competencia, lo que afecta tanto a la libertad de los usuarios como a la sostenibilidad de los sistemas democráticos.

Mirando hacia el futuro, es fundamental abordar estos retos con políticas de gobernanza de datos que garanticen la transparencia, la privacidad y la seguridad de la información, así como una regulación que limite los efectos negativos de la concentración de poder y promueva una democratización real del acceso a la tecnología y los datos. La ética y la responsabilidad en el uso de los datos serán aspectos cruciales para asegurar que los beneficios de la sociedad del dato se distribuyan equitativamente y que sus riesgos se gestionen de manera adecuada, evitando una vuelta atrás en la historia, hacia modelos neofeudales y limitaciones a las libertades y derechos de las personas, además de una potencial y grave pérdida del conocimiento acumulado durante siglos.

En definitiva, la sociedad del dato ofrece un horizonte de innovación y crecimiento, pero solo una gestión responsable y centrada en los valores humanos permitirá que los datos sean un recurso sostenible y beneficioso para todos, evitando que se conviertan en una herramienta de control y desigualdad e, incluso, en un arma de destrucción social y cultural.

## BIBLIOGRAFÍA

- [1] Flores-Galea, Antonio L. "Inteligencia artificial y sus implicaciones para los autores" (2022). ACTA, Vol. 131.
- [2] Mayer-Schönberger, Viktor, and Kenneth Cukier. "Big data: A revolution that will transform how we live, work, and think" (2013). Houghton Mifflin Harcourt.
- [3] O'neil, Cathy. "Weapons of math destruction: How big data increases inequality and threatens democracy" (2017). Crown.
- [4] Zuboff, Shoshana. "The age of surveillance capitalism" (2023). Social theory re-wired. Routledge, 203-213.
- [5] European Union. "General data protection regulation" (2016). Official Journal of the European Union 119: 1-88.
- [6] Morozov, E. V. G. E. N. Y. "To save everything, click here: the folly of technological solutionism" (2014). J. Inf. Policy 4.2014: 173-175.
- [7] Pentland, Alex. "Social physics: How social networks can make us smarter" (2015). Penguin.
- [8] Kitchin, Rob. "The data revolution: Big data, open data, data infrastructures and their consequences" (2014). Sage.
- [9] Floridi, Luciano. "The Fourth Revolution: How the infosphere is reshaping human reality" (2014). Oxford University Press.
- [10] Brynjolfsson, Erik, and Andrew McAfee. "The second machine age: Work, progress, and prosperity in a time of brilliant technologies" (2014). WW Norton & company.
- [11] Crawford, Kate, and Ryan Calo. "There is a blind spot in AI research" (2016). Nature 538.7625: 311-313.