OBS Business School



Los límites al uso de las tecnologías: ética y legalidad

Ramón Miralles
Profesor de OBS Business School

Noviembre, 2026

Partners académicos:

Universitat de Barcelona

unie Universidad



Autor

Ramón Miralles
Profesor de OBS Business School

Ramón Miralles es licenciado en Derecho por la Universidad de Barcelona, colegiado como ejerciente en el Ilustre Colegio de Abogados de Barcelona, con una experiencia profesional de más de 38 años en el sector de las TIC, dedicados fundamentalmente a dirigir proyectos de modernización digital en las administraciones públicas, primero en oficinas judiciales y después en la administración de la Generalitat de Catalunya y en el Ayuntamiento de Barcelona, asimismo destaca por su actividad en el ámbito empresarial, siendo actualmente Socio Director del Departamento de Privacidad, Compliance y Ciberseguridad en ECIJA Abogados, en Barcelona. Experto en sistemas de gestión de la seguridad de la información, y gestión de riesgos legales y tecnológicos, ha ocupado posiciones de CISO (seguridad de la información), CIO (tecnologías de la información) y CAE (auditoria), certificado profesionalmente en ámbitos de seguridad de la información y privacidad, y miembro de las juntas directivas de diferentes asociaciones profesionales. Profesor en diversos masters de formación permanente en OBS Business School: Ciberseguridad, Dirección de Sistemas y Tecnologías de la Información, Global Data Management, Machine Learning e Inteligencia Artificial y Tech MBA, así como en diversas Universidades y centros de estudios, en los que imparte materias relacionadas con los aspectos éticos y legales en el uso de las TIC. Ha participado activamente en proyectos relacionados con las tecnologías y la acción social, entre otros, en la consultoría TIC para el desarrollo del eje tecnológico del plan estratégico de la Defensa Pública de Costa Rica, en el contexto del programa Eurosocial II de la Comisión Europea, y en el grupo impulsado por la Red Iberoamericana de protección de datos, dedicado a la adecuación al derecho a la protección de datos de carácter personal en la acción humanitaria internacional. Ha recibido diferentes reconocimientos y premios: por el directorio internacional Best Lawyers, en sus ediciones 2022, 2023 y 2026, en el área de “Privacy & Data Protection Law”, y adicionalmente en la edición 2023 y 2026 premiado como "Lawyer of the Year" por su trabajo en el área de Privacy & Data Protection Law en Barcelona; premio colectivo de la Agencia Vasca de Protección de Datos 2018 al “Observatorio Iberoamericano de Protección de Datos”; y premio 2018 al profesor mejor valorado por los alumnos del plan de formación de la Asociación Profesional Española de Privacidad (APEP)

ÍNDICE DE CONTENIDOS

01 Introducción y contexto PÁG. 7

02 Derechos en la era digital PÁG. 11

03 Legislar los riesgos de las TIC y las complejidades del mundo digital PÁG. 16

04 Innovación y regulación: ¿Son compatibles? El impacto de la regulación en el uso de las TIC PÁG. 20

05 El desarrollo de marcos jurídicos relacionados con el uso de las TIC PÁG. 24

06 Estado global de la regulación de las TIC PÁG. 28

07 Inteligencia Artificial PÁG. 37

08 El uso ético de las TIC PÁG. 43

09 Conclusiones PÁG. 48

Prólogo

No anuncio ninguna novedad si afirmo que las tecnologías de la información y la comunicación (TIC) están intensivamente presentes en nuestro día a día, ya que usamos tecnologías en el ámbito profesional, educativo, familiar, de ocio, de consumo, solo por citar algunos de ellos.

En esencia, usamos "ininterrumpidamente" las TIC para comunicarnos, acceder a información y realizar muy diversas actividades o tareas, en definitiva, nos apoyamos en las tecnologías para mejorar la forma en que trabajamos, aprendemos y nos relacionamos, o al menos, así debería ser.

Antes de entrar en materia, quiero empezar con una declaración sobre el modo en que se ha preparado y realizado este informe, anunciando que **no he usado ningún asistente de inteligencia artificial para elaborarlo**, apoyándome en la IA exclusivamente para realizar algunas búsquedas de información, que posteriormente he contrastado con diferentes fuentes, para asegurar el rigor de la información analizada.

Este compromiso y ejercicio de transparencia no obedece a ninguna obligación legal o jurídica, es una postura ética, que parte del **principio de responsabilidad**, es decir: soy el único responsable de cualquier tipo de error y, por supuesto, también de los aciertos, si los hubiera, que puedan encontrarse en este informe.

Creo firmemente en que tecnologías como la inteligencia artificial pueden aportarnos grandes beneficios, siempre y cuando las usemos adecuadamente, y usarlas adecuadamente significa, en primer lugar, que no nos sustituyan o suplanten, y que sirvan para mejorar nuestro trabajo y no para hacer todo nuestro trabajo.

Según diversas fuentes consultadas, en el año 2018, Michihito Matsuda[1] fue candidato en las elecciones municipales de la ciudad de Tama (Tokio), representó al Partido Liberal Democrático de Japón, y obtuvo un meritorio tercer puesto, de entre 11 candidatos, a pesar de que era un robot y la inteligencia artificial con la que funcionan los actuales

[1] Inteligencia Artificial: La historia de Michihito, el robot que estuvo a punto de ser alcalde de una ciudad en Japón – FayerWayer

"chatbots" aún no estaba a su alcance. Todos estaremos de acuerdo en que no sería lo mismo tomar decisiones con la ayuda de Michihito, que dejar el gobierno en sus manos.

Hay un dato que resulta muy relevante, aunque las cifras puedan variar según la fuente consultada, y es que diversos estudios realizados entre 2025 y 2026 revelan que, como mínimo, el **50%** de la información que podemos encontrar en internet ha sido generada por la inteligencia artificial y, en algunos casos, se hacen previsiones de que en el 2026 podría llegar al **90%**[2].

Investigadores de Amazon Web Services cuantifican en un **57%**[3] el contenido creado o traducido por IA; al respecto hay que destacar que, por ejemplo, las traducciones automáticas de los sitios web mediante IA no están exentas de sesgos, por lo que no siempre la traducción responde al sentido del texto traducido.

El informe "AI Index Report 2026" de la Universidad de Stanford[4], también constata que menos del **50%** de los contenidos de internet han sido elaborados completamente por humanos, y en estudios citados en el índice, se determina que la cantidad de contenido sintético, es decir, creado por IA, se sitúa en el 51.7%.

Este hecho da pie a teorías como la "*Dead Internet Theory*"[5], que en síntesis sostiene que la actividad en **la red está siendo dominada por contenidos generados por IA, bots, y algoritmos**, quedando la presencia humana directa en un segundo plano, en definitiva, que en la web hay más actividad automatizada que humana, y es un fenómeno que seguirá en aumento.

Este escenario requiere plantearse qué consecuencias puede tener, y su gravedad, por ejemplo, y sin ánimo de ser exhaustivo, qué pasa con la calidad de la información disponible, con la falta de originalidad, con la creación de un pensamiento único o dirigido, con la suplantación

[2] El 90% del contenido de internet en 2026 será generado por inteligencia artificial

[3] ¿Está el 57% de Internet creado por IA? | Interactivity / Agencia de Marketing Online

[4] The 2026 AI Index Report | Stanford HAI

[5] La internet muerta es realidad: el 17% de internet es generada por IA - Digital Trends Español

de los humanos, con la desaparición del espíritu crítico, con la libre adquisición del conocimiento, con la distinción entre lo real y lo fciticio y aún más allá, **a donde nos lleva el hecho de que la IA se alimente de sí misma para seguir creando los contenidos que nos ofrece**, la pregunta final, o el dilema si se quiere plantear en términos éticos, es si queremos que la historia (nuestra memoria colectiva) y el futuro de la humanidad quede exclusivamente en manos de los algoritmos, o para ser más precisos, de quienes crean los algoritmos (sin perjuicio de que a su vez mucho de ellos ya estén creados por la propia IA) *¿Debemos evitarlo antes de que sea demasiado tarde?* (tal vez ya sea demasiado tarde) *¿Los humanos debemos recuperar el control?* Eso sí, con todas nuestras virtudes y muchos defectos.

La esperanza, o los medios para revertir lo que en mi opinión son consecuencias no deseables, en un alto grado tal vez se encuentre en las leyes y en la ética, aunque no exclusivamente.

En todo caso, mi postura o compromiso de no usar la IA en este informe, es solo una pequeña aportación al cambio de paradigma actual, en definitiva, no deja de ser un grano de arena en el desierto.

Por cierto, si se pregunta a un asistente de IA de uso general qué es un *"grano de arena en el desierto"*, os contestará que: *"Un grano de arena en el desierto es, literalmente, una diminuta partícula de roca o mineral. La mayoría de los granos de arena de los desiertos miden entre 0,06 y 2 milímetros y suelen estar formados principalmente por cuarzo, aunque su composición puede variar según la región"*, aunque al final, después toda una serie de explicaciones técnicas, añadirá a su respuesta que "*cuando alguien dice «soy solo un grano de arena en el desierto», quiere expresar que es una pequeña parte de algo mucho más grande",* eso espero ser yo.

Y también espero que este prólogo os anime a seguir con la lectura de este informe.

01

Capítulo 1.

Introducción y contexto



Los avances tecnológicos son una constante en la historia de la humanidad, como fruto de descubrimientos e invenciones, que tienen como denominador común el hecho de haber aportado evidentes ventajas para el propio desarrollo de la humanidad, provocando la mejora del bienestar de las personas, pero que a la vez **han generado nuevos riesgos o potenciados los ya existentes** o, en otros casos, ha implicado la necesidad de abordar retos de adaptación a las nuevas circunstancias derivadas de esos avances tecnológicos.

Hay multitud de ejemplos contemporáneos al respecto: la energía nuclear, la industria automovilística, la industria farmacéutica y de la salud, la aviación comercial, etc., simplemente por citar algunos entornos en los cuales ese binomio de "beneficio" y "riesgos" concurre sin lugar a duda.

En esos supuestos, el papel de la regulación, en forma de normas jurídicas, no ha sido otro que intentar mitigar esos riesgos mediante la incorporación de **principios, derechos y obligaciones**, es decir, la regulación cumple con su función de crear unas condiciones de convivencia aceptables, o de equilibrio, entre los diferentes intereses que pueden entrar en conflicto en diversas y variadas situaciones.

Suelo recurrir a la frase, *"la libertad permite a gente como usted hacer lo que le dé la gana y los derechos nos protegen a los demás de gente como usted"*, pronunciada por Robert De Niro en el papel de George Mullen en la serie "Zero Day", durante una conversación con una alta ejecutiva de una importante empresa tecnológica, porque resume a la perfección la necesidad de que existan normas que regulen el uso de las tecnologías.

Para ejemplificar lo hasta aquí expresado, quisiera describir brevemente el paralelismo entre la industria de las TIC y la industria automovilística, por lo que respecta a su desarrollo y a la necesaria regulación que ha ido acompañando a ese desarrollo, tanto desde la perspectiva de los riesgos (en particular, la seguridad), como de los retos empresariales que han tenido que abordar las organizaciones.

Según diversas fuentes, la primera víctima documentada de un accidente de tráfico relacionado con un vehículo a motor fue Mary

Ward, en 1869, que iba como pasajera en un vehículo a vapor; al parecer, en una curva perdió el equilibrio, se cayó al suelo y fue arrollada por el mismo vehículo en que viajaba.

Y en el 2018, por primera vez, un vehículo autónomo sin conductor atropelló a una persona, causándole la muerte a Elaine Herzberg, que murió a causa de las heridas sufridas después de ser atendida en un hospital.

Casi 150 años separan a ambos sucesos, pero **en ambos casos un avance tecnológico acabó causando la muerte a una persona**, porque el riesgo de que el daño causado pudiera llegar a producirse era intrínseco en ambos avances tecnológicos.

A finales del siglo XIX y principios del XX con el despliegue de la industria automovilística se empezó a regular la presencia de los automóviles en la vía pública, como consecuencia de los evidentes riesgos que, para la integridad física de las personas, estaban suponiendo.

En España, el 17 de septiembre de 1900 se aprobó la primera norma orientada a regular el tráfico y también empezó a plantearse la necesidad de regular y controlar el tráfico de vehículos a motor, mediante agentes públicos especializados, dedicados específicamente a esa tarea (los agentes de tráfico).

Las primeras regulaciones intentaban poner orden en la circulación, preservando la seguridad de conductores, pasajeros y peatones, para con el tiempo ir incidiendo en los aspectos relacionados con la seguridad activa y pasiva de los propios vehículos, e incluso, en décadas más cercanas, en relación al impacto medioambiental de los vehículos a motor.

El atropello de 2018 por un vehículo autónomo provocó que Uber suspendiera su programa de pruebas de vehículos autónomos en Estados Unidos y Canadá, pero además provocó que, a pesar de la presión de las compañías tecnológicas para que el Congreso estadounidense aprobará la legislación que debía acelerar la introducción de los coches autónomos en EEUU, varios congresistas demócratas bloquearon la ley, por sus dudas en torno a la seguridad de los sistemas relacionados con el uso de vehículos sin conductor.

Anthony Foxx, antiguo secretario de Transporte de los Estados Unidos entre el 2013 y el 2020, siendo Presidente Barack Obama, publicó en Twitter un mensaje en el que expresaba que lo que había sucedido era *"una llamada de aviso para toda la industria del vehículo autónomo y para el Gobierno para que pongan como prioridad la seguridad"*.

Los órganos legislativos de los países, con mayor o menor fortuna, suelen estar atentos a la realidad y a sus cambios, otra cuestión es el ritmo con que son capaces de regular nuevas realidades, por eso, la idea de que **el legislador va siempre por detrás de la realidad, se acentúa aún más cuando esa realidad está vinculada a las tecnologías de la información y la comunicación**, ya que la velocidad de su desarrollo y de los diversos retos y riesgos que supone, complican el hecho de elaborar marcos jurídicos sostenibles en el tiempo, que puedan satisfacer en cada momento todas las necesidades e intereses enfrentados, y en particular los riesgos que suponen para las personas.

Sin embargo, hay que subrayar que el hecho de que las leyes vayan por detrás de la realidad, no podemos considerarlo como algo negativo, al contrario, esa característica potencia la seguridad jurídica, ya que solo se regula lo que existe, y no situaciones excesivamente futuribles o inciertas, lo que si podemos valorar negativamente es la **lentitud del legislador a la hora de regular situaciones complejas**.

Por tanto, ese uso de las TIC tiene que ir necesariamente acompañado de **medidas que potencien la confianza en las tecnologías de la información y la comunicación**, a fin de desplegar al máximo sus beneficios, tanto para los ciudadanos a título individual, como para las empresas, y en general para el conjunto de la sociedad. En esa generación de confianza **tienen un papel muy relevante el conjunto de normas que regulan el uso de las TIC y un enfoque ético por parte de los desarrolladores y responsables** del despliegue de tecnologías.

02

Capítulo 2.

Derechos en la era digital



En 1948, cuando se adoptó la Declaración Universal de Derechos Humanos, la Asamblea General de la Organización de Naciones Unidas difícilmente podía imaginarse el papel y la importancia que ahora tienen las tecnologías de la información y la comunicación.

Ni tampoco, hasta qué punto los derechos humanos recogidos en la Declaración se podían ver afectados por los avances tecnológicos, no solo aquellos impactados de una manera muy evidente, como el derecho a la privacidad o a la libertad de opinión o expresión, sino también otros como el derecho a la libertad y a la seguridad personal, el derecho al libre desarrollo de la personalidad, al honor, o incluso la presunción de inocencia, ya que entre otros, estos también se ven fuertemente afectados por el uso de las tecnologías de la información y la comunicación y, en especial, de internet.

La incidencia sobre los derechos es diversa, por ejemplo, el derecho a la privacidad, entendido como el derecho a que no se produzcan injerencias arbitrarias en la vida privada, es evidente que con los avances tecnológicos se ve directamente amenazado.

Mientras que, por ejemplo, para la libertad de opinión y expresión, los avances tecnológicos han supuesto disponer de unos medios de expresión infinitamente más potentes que los que podían preverse en 1948 y que, por tanto, a priori podríamos considerar que, en general, disponemos de más mecanismos, y de mayor alcance, para expresarnos y hacer llegar nuestra opinión, tanto a título individual como colectivo, eso no quiere decir que no existan también amenazas para la libertad de expresión derivadas del propio medio tecnológico, por ejemplo, las derivadas de la censura de la red que ejercen algunos estados.

Desde mediados del siglo pasado las tecnologías de la información y la comunicación se han diseminado más allá de los centros de investigación, de las Universidades, de las grandes empresas y de las administraciones públicas, **desplegándose en las calles de nuestras ciudades, en los hogares y en los bolsillos de las personas** (incluso más allá, si pensamos en las tecnologías incorporadas en la ropa y complementos, o incluso si pensamos en los implantes de tecnología en seres humanos o en los “neuro-datos”).

Las tecnologías se han convertido en bienes de consumo, artículos de primera necesidad, casi irrenunciables para el desarrollo de las actividades económicas y sociales, al menos en los países desarrollados, pero incluso también en aquellos que están menos desarrollados.

Sin duda, el primer gran salto de las TIC fue el propiciado por internet, desde entonces nos hemos visto sorprendidos, casi a diario, con nuevas y cada vez más seductoras y deslumbrantes soluciones tecnológicas que, sin duda, nos facilitan nuestro día a día, no solo en lo profesional, también en lo personal.

Las tecnologías de la información y la comunicación no han traído consigo exclusivamente avances en positivo, ya que también conllevan amenazas y riesgos para los individuos y las organizaciones, especialmente en el contexto de la privacidad y de la protección de información de todo tipo.

Ya en 1890, los juristas Samuel Warren y Louis Brandeis, en su artículo "The Right to Privacy", publicado en la "Harvard Law Review", alertaban de hasta qué punto los avances tecnológicos de la época ponían en peligro la vida privada, cuando escribieron que: *«Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y para garantizar al individuo lo que el juez Cooley denomina el derecho "a no ser molestado".»*

Más recientemente, en el 2001, el periodista norteamericano Edwin Black publicó su libro "IBM y el holocausto", en el que describe la alianza estratégica entre la Alemania nazi y la conocida multinacional de tecnologías de la información, que en aquel momento sirvió de base para el uso de máquinas, todavía pre-informáticas (año 1933), para realizar el censo de la población alemana en un tiempo récord, información que, según describe el autor, fue utilizada en buena parte para el control de las personas y otras acciones que infringieron daño y muerte a muchas personas.

En su introducción el autor hace una afirmación tan reveladora, como inquietante, por su extraordinaria actualidad:

«La humanidad apenas notó el nacimiento silencioso del concepto "información organizada masivamente", que se convirtió en un medio de control social, un arma de guerra y un camino para la destrucción de la gente.»

En el ensayo "The Laws of Cyberspace"[6], que Lawrence Lessig[7] presentó en la conferencia Taiwan Net'98, celebrada en Taipei, en marzo de 1998, hizo una primera aproximación al papel y características de las leyes en el denominado "ciberespacio".

Hay que tomar consciencia de que el mundo (la realidad que nos rodea) está compuesto por un espacio presencial, aquel en el que las relaciones entre personas y resto de agentes de la sociedad (estado y personas jurídicas) se desarrolla en el plano físico, y un espacio virtual ("ciberespacio"), en el que las relaciones entre esos agentes se desarrollan en un espacio lógico, a efectos ilustrativos coexisten un mundo de los "átomos" y un mundo de los "bits".

En palabras de Lessig: *«El ciberespacio tiene el potencial de ser el espacio más plena y extensamente regulado que hayamos conocido jamás en cualquier lugar y en cualquier momento de nuestra historia. Tiene el potencial de ser la antítesis de un espacio de libertad.»*

Las reflexiones de Lessig debemos conectarlas con la teoría sobre los derechos humanos, en particular los calificados como **derechos de cuarta generación**, que si bien la doctrina no termina de ponerse de acuerdo en cuál sería su contenido y características, algunos autores hacen referencia a que los derechos de cuarta generación tendrían en común asegurar a todos los individuos el acceso a las tecnologías de la información y la comunicación, considerando que el paradigma de la sociedad de la información y del conocimiento, obliga a ello.

Siguiendo esa línea doctrinal, en esa teórica cuarta generación se incluirían, entre otros: el derecho de acceso a la informática, el derecho al acceso a la sociedad de la información en condiciones de igualdad, al uso de las infraestructuras de telecomunicaciones, a la formación en

[6] The Laws of Cyberspace

[7] Lawrence Lessig - Harvard Law School | Harvard Law School

las nuevas tecnologías, a la autodeterminación informativa, al “Habeas Data” o a la seguridad digital.

Con independencia del enfoque teórico, lo cierto es que las tecnologías de la información y la comunicación y el uso de internet, pueden facilitar y potenciar todos los derechos, pero también pueden limitarlos.

En este nuevo paradigma, todas las libertades y derechos de la humanidad están presentes en el espacio digital, lo que conlleva necesariamente a su reconocimiento y salvaguarda por parte del Estado de Derecho, cuestión que evidentemente constituye un complejo reto para los sistemas jurídicos, que han empezado reconociendo tímidamente en algunas leyes, lo que se ha venido en denominar derechos digitales.

03

Capítulo 3.

Legislar los riesgos de las TIC y las complejidades del mundo digital



Los riesgos que tienen su origen en el uso de las TIC pueden ser una primera motivación para que el legislador decida actuar, en el momento en que tales riesgos empiezan a manifestarse, para ello **el legislador recurre a aplicar un enfoque al riesgo** cuando decide adoptar este tipo de normas, trasladando a quienes deben cumplirlas la obligación de tener en cuenta el riesgo que genera el uso de las TIC y, en consecuencia, obligándoles a tomar las decisiones más adecuadas para mitigarlo.

Debemos tener en cuenta que la única manera de eliminar el riesgo es dejar de hacer aquello que lo produce, por tanto, este tipo de leyes que regulan el uso de las TIC obligan a analizar los riesgos y a adoptar medidas para minimizarlos, llegando incluso, en algunos casos, a prohibir determinados usos de esas tecnologías, por considerar que suponen un riesgo inaceptable, ya que no existen medidas efectivas para mitigarlo.

Regular el uso de las TIC no está exento de complejidades, en mi opinión hay al menos 5 variables que nos van a permitir tomar conciencia de lo complicado que puede ser tener leyes que regulen adecuadamente el uso de la TIC, cuando convivimos en un escenario sociedades altamente tecnificadas y extensamente conectadas, incluso en países o zonas geopolíticas en vías de desarrollo:

- **La primera variable a tener en cuenta es la rápida evolución de las tecnologías y de su uso, a un ritmo que difícilmente pueden seguir los legisladores, al menos con los mecanismos tradicionales de regulación, asalta aquí la duda de si tal vez deberíamos pensar en adaptar las técnicas legislativas, es decir: ¿Se podría legislar de otra manera?** O al menos **¿De una manera más rápida?**

- La **extraordinaria capacidad de procesamiento de la información**, cuantitativa (volumen de información) y cualitativa (diferentes tipos de informaciones), que ha puesto a nuestro alcance soluciones tecnológicas prácticamente para todo, lo que nos ha puesto en una situación de alta dependencia de las TIC, incluso provocando problemas de “tecno-adicción”, pensemos en aquellas situaciones en la que nos sorprende una falta de acceso a internet,

o cuando no podemos enviar mensajes por nuestra aplicación de mensajería instantánea preferida, ya sea por un incidencia técnica o por un ciberataque, situaciones que como mínimo nos causan incomodidad y, en algunos casos, incluso angustia por no estar comunicados, y ya no digamos cuando ese incidente afecta al uso que las empresas hace de las TIC, que puede traducirse en pérdidas millonarias o de reputación.

- También añade complejidades **el hecho de que la información tenga un valor económico**, no solo desde la perspectiva de la compraventa de información (sea en base a un comercio lícito o ilícito), también como medio productivo, de manera que la información constituye un verdadero activo empresarial que debe ser protegido y estar disponible, ya que de él depende el negocio, pensemos en nuestras bases de datos de clientes, de pedidos o en las fotos de familia que tenemos almacenadas en la nube.
- Asimismo, la relación entre desarrollo y despliegue de las tecnologías de la información y la comunicación, y el progreso económico, es una relación que debe tenerse muy en cuenta a la hora de elaborar y aprobar leyes, ya que **poner excesivas barreras a la innovación puede implicar poner freno al desarrollo económico**, lo cual es una cuestión clave desde una perspectiva política y social, y encontrar el equilibrio no siempre es sencillo, ya que los intereses y derechos en juego son muchos, y todos ellos ejercen presión sobre el legislador, para que legisle en su favor.
- Y, finalmente, la **globalidad del entorno digital**, lo que conlleva la desaparición de las fronteras físicas y las dificultades que ello puede suponer, en particular, para la determinación de las leyes aplicables, la jurisdicción competente y la ejecución de las resoluciones judiciales, cuando un mismo negocio digital puede implicar la concurrencia de diversos operadores (comprador, vendedor, transportista, proveedores de telecomunicaciones, sitios web, etc.), cada uno de ellos establecidos en distintos países.

A toda esta complejidad del entorno digital, se une el hecho de que las relaciones laborales, interpersonales, educativas, de ciudadanía, de negocio, etc., se despliegan tanto en el plano presencial como

en el plano lógico o virtual, de manera que la realidad finalmente está formada por la suma de ambos espacios, con intersecciones en diversos puntos, que al final **dan lugar a una nueva y única realidad de "bits" y "átomos"**, extraordinariamente complicada.

04

Capítulo 4.

Innovación y regulación: ¿Son compatibles? El impacto de la regulación en el uso de las TIC



En general los Estados de derecho asumen, o deberían asumir, el papel de fomentar el desarrollo económico y el bienestar de los ciudadanos y, en tanto la innovación puede favorecer ese objetivo, el apoyo a la innovación ha sido incluido en las estrategias públicas, y por tanto en las agendas políticas y de regulación.

Al fin y al cabo, compatibilizar innovación y regulación no debería ser tan complicado, cabe en este punto hacer referencia, por ejemplo, a lo que podemos considerar **uno de los primeros ejemplos de norma reguladora de la incorporación de nuevas tecnologías** en la actividad administrativa en España, la Real Orden de 12 de febrero del año 1900, que con una sencilla regulación establecía la admisión, por parte de las administraciones públicas, de **escritos hechos con máquina de escribir**, equiparándolos a los presentados en forma manuscrita, que era como hasta entonces se presentaban los documentos dirigidos a las administraciones públicas.

«Considerando que no existe ninguna razón administrativa ni de otra índole que aconseje no admitir las instancias y demás documentos hechos con máquina de escribir, siendo más clara y fácil su lectura que muchos de los escritos a mano, y cuya legalidad consiste en la autenticidad de la firma que los suscribe y no en que estén hechos precisamente con letra manuscrita.

S.M. el REY (Q.D.G.), y en su nombre la REINA Regente del Reino, ha tenido a bien disponer que en todas las oficinas del Estado, provinciales y municipales se admitan cuantas instancias y documentos se presenten hechos con máquinas de escribir, en los mismos términos y con iguales efectos de los escritos o copiados a mano.»

La innovación se ve afectada e impactada por **la regulación, ya que esta debe sujetarse al ordenamiento jurídico en sus diferentes fases de desarrollo**, por tanto, los Estados, en su papel de regulador, influyen sobre la actividad innovadora, hasta tal punto que **la puede inducir o dificultar**, por tanto, **la regulación no va a ser neutra** respecto del desarrollo de las actividades vinculadas a la innovación.

La relación entre innovación y regulación no está exenta de cuestiones que pueden ser críticas, ya que no debemos perder de vista que se trata

de una relación de carácter dinámico, de tal modo que las variables del entorno y la casuística concreta va a incidir directamente, y en cada momento, en el impacto positivo o negativo, que la regulación vaya a tener en la innovación.

El equilibrio está en conseguir que la regulación no sea un obstáculo a la innovación, y que a la vez ello **no suponga la devaluación de derechos y libertades** de los ciudadanos, de los cuales el Estado es garante en última instancia, y que, a su vez, permita propiciar el crecimiento económico y el bienestar social, objetivos todos ellos compatibles si se consigue elaborar una regulación adecuada.

La conocida como *"hipótesis de Porter"*[8] parte de la base de que **la regulación social induce a la innovación y eleva la competitividad de las empresas e industrias**, ya que en muchos casos obliga a mejorar el uso eficiente de los recursos o a aumentar la calidad de los productos.

En general, los estudios de análisis del impacto de la regulación sobre la innovación distinguen entre 2 tipos de innovación, según el beneficiario; por un lado **la "innovación social"**, relacionada con innovaciones en productos o procesos que generan beneficios sociales, pero que no implican una rentabilidad directa para las empresas (por ejemplo: no contaminar el agua o el aire, la gestión de residuos, o **las medidas de seguridad relacionadas con la protección de los datos de carácter personal**), y por otro, tenemos la denominada **"innovación de mercado"**, en este caso sí que la innovación puede generar beneficios para las empresas, a través de la venta de bienes y servicios a los que se ha aplicado innovación.

Si nos fijamos en casos concretos, y siguiendo con el símil de la industria automovilística, esta ha ido innovando desde sus inicios, pasando de una situación en la que no existía ningún tipo de

[8] De la Wikipedia: *"**Michael Eugene Porter** (n. 1947, Ann Arbor, Michigan) ostenta la cátedra Bishop William Lawrence en la Escuela de Negocios Harvard (HBS) y dirige el Institute for Strategy and Competitiveness de la misma escuela de negocios. Es una autoridad globalmente reconocida en temas de estrategia de empresa, consultoria, desarrollo económico de naciones y regiones, y aplicación de la competitividad empresarial a la solución de problemas sociales, de medio ambiente y de salud."*

regulación, a ser un sector altamente regulado, que afecta a todos los agentes implicados, desde el fabricante al usuario final, pasando por los diferentes intermediarios y proveedores relacionados con la industria del automóvil, **una regulación intensa y muy completa, que en ningún caso ha impedido la innovación en ese sector productivo, que sigue innovando en diferentes direcciones** (seguridad, energía, consumo, comodidad, diseño, vehículo conectado, etc.).

En resumen, la regulación sin duda va a impactar en el modo en que vayamos a desarrollar y usar las tecnologías de la información y la comunicación, por tanto, en la toma de decisiones sobre su desarrollo y uso hay que tener en cuenta las exigencias jurídicas que nos planteen las normas que apliquen a cada caso.

05

Capítulo 5.

El desarrollo de marcos jurídicos relacionados con el uso de las TIC



Los sistemas de información, y los diferentes elementos que los componen, constituyen verdaderos activos de las organizaciones, que son valiosos para el desempeño de sus actividades.

El enfoque a riesgos en la toma de decisiones sobre el uso de las TIC, va a ser clave para adoptar las decisiones más adecuadas para el contexto de cada organización, teniendo en cuenta sus actividades y sus prioridades, y con el fin último de que las actividades de negocio o de servicio no se vean comprometidas, ahora bien, esa protección y esos riesgos no se centran exclusivamente en la propia organización, ya que la regulación del uso de las TIC **suele centrarse principalmente en proteger a las personas**, ya sea directamente, o de manera indirecta protegiendo los servicios y aplicaciones de las que son usuarios.

Las decisiones sobre el diseño, implementación y uso de las TIC están supeditadas a 2 cuestiones: (i) conseguir sistemas de información e infraestructuras que den respuesta eficaz, eficiente y segura a las necesidades de cada organizació y (ii) cumplir con las normas jurídicas que sean de aplicación, bien con carácter general, o en el marco de una actividad concreta (servicios financieros, seguros, administraciones públicas, suministros de energía, comercio electrónico, marketing digital, etc.).

En lo que se refiere al uso de las tecnologías de la información y la comunicación existen muy diversas normas jurídicas que deberán ser tenidas en cuenta, ya sea porque establezcan claramente obligaciones de protección de la información; o bien, porque describen actividades de tipo delictivo en las que las empresas pueden verse involucradas, ya sea por actuar como víctimas, o como agresores; o que regulen la prestación de servicios digitales; o que obliguen a adoptar medidas en relación a la ciberseguridad, el teletrabajo, etc., por citar tan solo algunos ejemplos.

Desde un punto de vista competitivo, cada vez más, una empresa que cuida de sus sistemas de información no solo va a desarrollar con mayor eficacia sus procesos operativos, **también va a generar mayor confianza en sus clientes y empleados**, y en general en todas aquellas partes interesadas en su actividad, lo que sin duda le puede generar un valor competitivo en el mercado, especialmente si los competidores no

tienen en cuenta ambas esferas de decisión: **la operativa**, que tienen que ver con uso eficaz y eficiente de los recursos tecnológicos, **y la jurídica**, que obliga a cumplir con una serie de requisitos cuando se utilizan las TIC, que es de lo que se ocupa este informe.

En estos momentos para las organizaciones realmente digitales, el hecho de poseer información prácticamente no tiene valor, con la excepción de aquellas que se dedican exclusivamente a comerciar con información, aun así, tal información también deberá ser objeto de procesamiento para su comercialización, con el fin de estructurarla y depurarla.

Lo que realmente tiene valor, es hasta qué punto se tiene una capacidad real de analizar la información, mediante tecnologías que si bien cada vez son más complejas en cuanto a su diseño, también son más efectivas y eficientes, y de sencilla implementación, aportando mejores resultados y, en consecuencia, un mayor valor para las organizaciones, aunque **un mal uso de estas puede llegar a impactar muy negativamente en las personas**.

Por ello, los marcos jurídicos están regulando todo tipo de información y todas las posibles opciones de procesamiento de la información que aportan las tecnologías de la información y la comunicación, **ocupándose particularmente de regular las tecnologías más emergentes o disruptivas**, a fin de aportar seguridad jurídica y garantías de protección para los derechos y libertades de las personas que puedan verse expuestos a los riesgos derivados de ese procesamiento de la información y, lo que es más relevante, de los resultados y acciones sustentadas en el conocimiento obtenido de la información.

Realmente no existe una regulación como tal de Internet, es decir, **no existe un marco jurídico que regule de una manera uniforme cómo debe ser Internet, o lo que sucede en Internet**, sino que existen diferentes conjuntos de normas (marcos jurídicos), que se ocuparan de establecer las reglas de los diferentes usos de las TIC que, con carácter general, van a tener como denominador común su conexión a la Red.

Internet no deja de ser una infraestructura de comunicaciones, que facilita que se lleven a cabo multitud de actividades diferentes, y aunque el protocolo de comunicaciones[9] que utiliza se creó pensando en conectar máquinas, realmente los impactos finales de esas actividades (positivos y negativos) afectan a las personas, de ahí la **necesidad de regular lo que sucede en la Red**.

Que no exista un marco jurídico específico que regule Internet no quiere decir que no esté gobernada, por supuesto existen un marco de normas, que permiten que internet funcione con un cierto orden; en primer lugar, hay normas de carácter técnico (no entraremos aquí a describirlas), que se complementan con un modelo de **"gestión administrativa"** que hace que la red funcione y se desarrolle en un "framework" controlado respecto de su funcionamiento técnico; otra cuestión son los **contenidos y servicios que circulan por la Red, que son los que realmente y a efectos prácticos van a generar conflictos de tipo jurídico**.

La UNESCO promueve *"un enfoque abierto, transparente e inclusivo de la gobernanza de Internet"*, que incluye *"la libertad de expresión, el respeto de los derechos humanos y la privacidad, el acceso universal y la interoperabilidad técnica"*; además, le preocupan cuestiones como *"la ética, así como el respeto por la diversidad cultural y lingüística en el ciberespacio"*.

En definitiva, **no existe un marco jurídico global que establezca normas sobre los derechos y obligaciones relacionados con el uso de las TIC, ni de Internet**, lo que existe son normas aprobadas en cada país, o zona geopolítica, que regulan el uso de las tecnologías, desde muy diferentes puntos de vista.

[9] Los protocolos básicos que se usan en la transmisión de datos en internet son TCP (Protocolo de Control de Transmisión) e IP (Protocolo de Internet), a lo que de manera común nos referimos como TCP/IP; tales protocolos van a ser esenciales para que los dispositivos que acceden a la red (internet) se pueden comunicar, y que junto con otros protocolos de servicios forman lo que conocemos como internet.

06

Capítulo 6.

Estado global de la regulación de las TIC



Prácticamente todos los países han regulado cuestiones relacionadas con el uso de las TIC, se trata de regulaciones que, en general, suelen ser bastante neutras, por el propio objeto que regulan, sin perjuicio de que existan diferencias, que básicamente dependen de qué es lo que pone el legislador en el centro de la regulación: **a las personas, o las organizaciones** (y sus actividades).

En Europa, en general encontraremos un enfoque regulatorio centrado en **proteger a las personas**, mientras que en los Estados Unidos la regulación se centra más en la **actividad de las organizaciones**, pero esto no quiere decir que se centren en ello exclusivamente, si no que el peso de los obligaciones y derechos se enfocan hacía uno u otro objeto de protección, en otros casos, como por ejemplo China, la regulación **pone en primer lugar al Estado**, pero evidentemente, todo este tipo de normas protegen a personas, organizaciones y Estados, aunque se centren más en uno u otro aspecto.

Otras zonas geopolíticas desarrollan sus marcos jurídicos inspirándose en alguna de las tendencias existentes, por ejemplo, en Latinoamérica está muy presente el efecto Bruselas en determinadas regulaciones, por el cual las normas de la Unión Europea tienden a convertirse en estándares globales.

Como decía, los marcos jurídicos relacionados con el uso de las TIC abordan muy diversas cuestiones, sobre las cuales a continuación haré una breve referencia:

a. **Servicios digitales y mercado digital:** este ámbito de regulación se puede plantear desde dos perspectivas, como regulaciones parciales, que mediante normas concretas se van regulando aspectos que cada país considera que deben ser objeto de regulación, o bien obedeciendo a una estrategia más global, que tenga en cuenta no solo la resolución de conflictos presentes, si no también que sienten las bases de auténticos mercados digitales, en los que los datos forman parte de la economía y los servicios digitales den respuesta a las necesidades de los consumidores y usuarios, en un entorno seguro tanto desde la perspectiva jurídica como tecnológica, este último es el típico modelo de regulación Europea basado en estrategias específicas.

Por ejemplo, la *"Estrategia Europea de Datos"* responde al planteamiento de convertir a la UE en una sociedad en la que los datos sean esenciales en la toma de decisiones; esa estrategia incluye la creación de un mercado único de datos, con el objeto de que los datos circulen libremente por la UE entre diferentes sectores de actividad (públicos y privados), de manera que de ello se deriven beneficios directos para los ciudadanos, las empresas, los investigadores y las administraciones públicas.

b. **La protección de los datos personales:** posiblemente este tipo de regulación sea una de las más conocidas y desarrolladas del mundo. El derecho a la protección de los datos personales se puede considerar que por primera vez empezó a plantearse como derecho en Alemania, en los años setenta, y el principal motivo del legislador para elaborar una regulación que contemplara el control por parte de las personas sobre los datos personales propios, fueron **los avances tecnológicos** que, en relación a la informática, se estaban produciendo, y los riesgos que ello podía suponer para las personas, si se hacía un mal uso de sus datos personales.

Un denominador común que encontraremos en este tipo de regulación es que todas ellas regulan la seguridad de la información que, desde la perspectiva de protección de datos personales, implica concretar qué controles o medidas de seguridad hay que implantar en los sistemas de tratamiento de datos personales, a fin de preservar la disponibilidad, integridad y confidencialidad de la información de carácter personal de que disponen las organizaciones para el desarrollo de sus actividades.

El conjunto de la normativa de protección de datos se basa en la existencia de unos **principios** que deben ser aplicados en el tratamiento de los datos de carácter personal, que se completan con una serie de **obligaciones** concretas para aquellos que tratan los datos, y en unos **derechos** para los titulares de los datos personales que van dirigido a que las personas puedan controlar qué se hace con sus datos.

c. **La protección de los activos de información y de activos intangibles:** la "ciberinseguridad" en el entorno digital ha obligado a los legisladores a elaborar normas que promuevan la **cultura de la seguridad de la información y en general de protección de los activos y servicios digitales**, a veces de una manera "dolorosa", ya que en algunos casos se recurre incluso a la sanción económica (multa), ante el incumplimiento de obligaciones relacionadas con la protección de la información, especialmente en el caso del derecho a la protección de los datos de carácter personal o de las leyes de ciberseguridad, entre otros.

Los Estados han identificado claramente la necesidad de dotarse de una regulación que consolide y refuerce un escenario de **seguridad y confianza** para todos los agentes implicados en el uso de las tecnologías de la información y la comunicación.

Se trata de normas que, en general, se dirigen a proteger a las personas, bienes y servicios, obligando a analizar los riesgos de seguridad y, a aplicar medidas de seguridad adecuadas en los datos, procesos, aplicaciones, sistemas operativos, el "hardware", las comunicaciones, los soportes de información, las instalaciones físicas, etc., en definitiva, en todos los elementos involucrados en el funcionamiento de los sistemas de información.



La ciberseguridad ha pasado a ser una obligación jurídica, y a tener la consideración de un **bien jurídico que debe ser protegido**, ya que el actual paradigma de uso de las TIC no se concibe fuera de las redes públicas de comunicaciones, es decir, de Internet, por lo que difícilmente encontraremos sistemas de información que no estén conectados a la Red, o al "ciberespacio", de ahí que hablar de seguridad de los sistemas de información, a la práctica es referirse a la "ciberseguridad", o lo que es lo mismo a la protección de los activos de información accesibles desde o hacía Internet.

A pesar del fenómeno global que suponen los ciberataques, lo cierto es que a nivel internacional el desarrollo de normas jurídicas orientadas a imponer obligaciones en materias de ciberseguridad, u otras obligaciones de implementación de medidas de seguridad, es **muy desigual**, para profundizar en esta cuestión recomiendo los informes "Estado de la Ciber-Inseguridad: realidades y percepciones"[10] (2024) y "La Ciberseguridad desde un enfoque normativo"[11] (2025).

La realidad es que la información que manejan las empresas en sus sistemas de información está altamente expuesta a acciones de carácter delictivo, directa o indirectamente relacionadas con las tecnologías, de hecho casi a diario podemos leer noticias en prensa al respecto, se puede decir que **ninguna compañía está a salvo de ser el blanco de este tipo de violencia digital** y debe tenerse muy en cuenta que los objetivos de los delincuentes no se centran exclusivamente en las grandes compañías, o en empresas con datos valiosos (por ejemplo, bancos o grandes comercios electrónicos), **también son objetivo las pequeñas y medianas empresas, e incluso los particulares**.

Además, se pueden dar casos en que la propia empresa se convierta en un "agresor", cometiendo este tipo de delitos, por eso el ordenamiento jurídico de muchos países contempla esta posibilidad, por ejemplo, en España, que a partir de la reforma del código penal (primero en el 2010, completada posteriormente en el 2015) se ha incorporado la **responsabilidad penal de las personas jurídicas**, es decir, las

[10] Informe OBS: Estado de la Ciber-Inseguridad | OBS Business School

[11] Informe OBS: España y su normativa de ciberseguridad

empresas pueden llegar cometer delitos relacionados con el uso de las TIC y ser condenadas por ello.

En cualquier caso, las empresas están obligadas a articular mecanismos para defenderse, tanto de las acciones delictivas que van contra ellas, que habitualmente provienen del exterior, pero que a veces pueden tener un apoyo interno; como de la comisión de delitos por parte de la propia empresa.

La cibercriminalidad abarca diversas conductas delictivas, como los delitos de descubrimiento y revelación de secretos (que incluye acciones relacionadas con el "sexting"), de daños informáticos, de pornografía infantil, los delitos contra la propiedad intelectual, los delitos de terrorismo o los delitos de odio.

En toda esta materia resulta esencial tener en cuenta la existencia del *"Convenio sobre la ciberdelincuencia"*, de 23 de noviembre de 2001, del Consejo de Europa, conocido como el "Convenio *de Budapest"*[12] (ratificado por España y otros muchos países, no solo europeos); el citado Convenio incluye una **clasificación de los delitos informáticos**, que comúnmente se utiliza para abordar las cuestiones relacionadas con esas conductas.

En paralelo a la regulación de los "ciberdelitos", los cuerpos y fuerzas de seguridad de los estados han tenido que adaptarse a estas nuevas actividades delictivas, adquiriendo nuevos conocimientos y organizándose adecuadamente para llevar a cabo la lucha contra la ciberdelincuencia, que tiene un "modus operandi" propio, al menos por lo que respecta a la comisión material de los delitos, si bien, en los aspectos organizativos no dejan de actuar de manera equivalente a cualquier otro tipo de delincuencia organizada.

Otro aspecto que también es objeto de regulación es la **protección de la propiedad intelectual e industrial**, que se ve expuesta en el contexto digital desde diferentes perspectivas.

[12] BOE-A-2010-14221 Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.



La propiedad intelectual e industrial están directamente relacionadas con las creaciones de la mente humana[13], a las que **jurídicamente se las puede llegar a considerar un derecho patrimonial**, que es de carácter territorial y de exclusividad.

Las normas de los países en que se reconocen estos derechos, los otorgan por un tiempo determinado, durante el cual se pueden usar o explotar las invenciones o innovaciones protegidas, ya sea de manera comercial y/o industrial. La posibilidad de registrar esos derechos refuerza su protección.

Los derechos de propiedad intelectual e industrial también permiten obtener una protección jurídica eficaz para los denominados activos intangibles (por ejemplo, contenidos digitales), de manera que se refuerzan y aumentan las posibilidades de comercializar productos y servicios por parte de las organizaciones que invierten en su investigación y desarrollo.

[13] Este aspecto ha abierto el debate de que las creaciones mediante IA no estarían protegidas por estos derechos.

La irrupción de las tecnologías digitales ha cambiado la manera en que se producen y distribuyen los contenidos creativos, así como el acceso a los mismos[14], en el caso de la Unión Europea existen varas Directivas y Reglamentos que regulan los derechos de autor.

En Europa, los derechos de autor permiten que los profesionales o creadores[15] en los ámbitos de *"la escritura, la composición musical, el arte y el cine"*, entre otros, puedan **obtener una retribución por su obra, así como la protección de sus creaciones.** Otro tipo de creaciones que también pueden llegar a protegerse son los **programas informáticos y las bases de datos.**

Pero la regulación con fines de protección no queda solo en estas cuestiones, en este mismo ámbito de protección de los activos de información, también debe tenerse en cuenta la existencia de normas relacionadas con la **protección de infraestructuras consideras críticas**, así como la **protección de las telecomunicaciones**.

Se trata de ámbitos en los que con carácter general las organizaciones y usuarios no tienen que asumir la iniciativa en cuanto a obligaciones jurídicas de protección de los activos de información (excepto si deben asumir obligaciones jurídicas por el hecho de operar determinados servicios críticos o de telecomunicaciones), en este caso, las organizaciones y los usuarios suelen ser beneficiarios de esa protección que prevén las normas.

El objetivo final de este tipo de normas es que las entidades que operan servicios e infraestructuras críticas refuercen su capacidad de **"prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación y recuperación"**, ante los incidentes que puedan impactar negativamente en la prestación de servicios esenciales, concretamente, las entidades que explotan las citadas infraestructuras han de estar preparadas *"para hacer frente a los riesgos*

[14] Las normas de propiedad intelectual e industrial se han ido adaptando a la era digital, por ejemplo, respecto de la producción de dibujos y modelos, que se ha adaptado a causa de las impresoras 3D o a la irrupción de la inteligencia artificial.

[15] Derechos de autores, artistas intérpretes o ejecutantes, productores y organismos de radiodifusión.

para sus operaciones que puedan dar lugar a una perturbación en la prestación de servicios esenciales".

Respecto de lo anterior, se considera que las entidades críticas se enfrentan a un escenario *"dinámico de amenazas"*, entre las que se encuentran las *"amenazas híbridas y terroristas"*, que están en continua evolución, a lo que se une la **cada vez mayor interdependencia entre infraestructuras y sectores** (pensemos en la guerra en Ucrania o en el conflicto del Golfo Persico, y la crisis del gas, petróleo electricidad o del grano, con impactos en Europa y a nivel internacional).

A todo lo anterior, debe añadirse que, tal y como ya se ha analizado, el uso de las tecnologías de la información y la comunicación por parte de las organizaciones implica necesariamente el acceso desde sus redes privadas a redes públicas de telecomunicaciones (y también a la inversa); ese acceso resulta inevitable, en tanto que imprescindible, para el uso eficaz y eficiente de las TIC, hay que reiterar que hoy por hoy **no se podría concebir el uso de sistemas de información que no estén conectados a la Red.**

Por tanto, la disponibilidad de la red, y la seguridad de la propia red, desde la perspectiva del transporte de información (protección de origen, contenido y destino de las comunicaciones), resultan **esenciales y consustanciales a la propia prestación de los servicios de redes públicas de telecomunicaciones**.

En este sentido, **las infraestructuras de telecomunicaciones son críticas**, de manera que ante un incidente que impida su uso, la actividad de un país puede llegar a paralizarse seriamente.

07

Capítulo 7.

Inteligencia Artificial



Mención especial merece la regulación del uso de la inteligencia artificial, ya que en un contexto de avances tecnológicos acelerados y de creciente integración de la inteligencia artificial en diversos sectores, es imprescindible contar con una normativa que garantice **la seguridad, la transparencia y el respeto a los derechos fundamentales** en el desarrollo y uso de la IA.

Además se hace necesario referirse al Reglamento de Inteligencia Artificial europeo, ya que es una iniciativa legislativa pionera[16] que tiene por objeto establecer un marco normativo armonizado para el desarrollo, despliegue y utilización de sistemas de inteligencia artificial (IA) dentro de la Unión Europea, su existencia tiene **implicaciones legales para los diferentes agentes que intervienen en el mercado a la IA, desde los responsables del desarrollado de la IA, hasta quienes actúan como responsables de su despliegue, pasando por proveedores, comercializadores, en incluso para los usuarios finales.**

El alcance transversal de la IA como tecnología aplicable a múltiples productos y servicios, hace que necesariamente deba interactuar con otras normas, en particular con las de privacidad y protección de datos personales y la regulación de datos no personales, cuando los datos se usen en cualquiera de las etapas del ciclo de vida de los sistemas de IA.

El citado reglamento de IA es una iniciativa legislativa que se enmarca en los esfuerzos por actualizar y **adaptar el marco regulatorio de la Unión Europea a los avances tecnológicos**, proporcionando claridad legal y previsibilidad para los desarrolladores y usuarios de sistemas de IA, y estableciendo las bases para una cooperación efectiva entre los Estados miembros y las instituciones de la UE en la supervisión y cumplimiento de las normas.

La inteligencia artificial se ha convertido en una tecnología transformadora, que impulsa la innovación y el crecimiento en numerosos sectores económicos y sociales. Su rápida evolución y adopción plantea desafíos significativos en términos de regulación

[16] Existen otras iniciativas de tipo legislativo o equivalente que se platean regular la IA, si bien, por su alcance e impacto la regulación europea es sin duda las más madura y completa.

y control, especialmente en lo que respecta a la protección de los derechos fundamentales, la seguridad y la privacidad de los individuos.

El Reglamento de IA forma parte de una estrategia digital más amplia de la UE, que tiene como objetivo fomentar la innovación y garantizar **que Europa mantenga su competitividad en el ámbito tecnológico global**. Al mismo tiempo, se busca proteger a los ciudadanos y empresas europeas de los posibles perjuicios que podrían derivarse del uso indebido de los sistemas de IA, ya que pueden tener un impacto directo en derechos como **la privacidad, la no discriminación, la libertad de expresión, la protección de datos personales y el derecho a un juicio justo**, entre otros.

Otro aspecto a tener en cuenta es que la IA tiene el potencial de perpetuar, amplificar o incluso crear, sesgos y discriminaciones. El Reglamento exige que los sistemas de IA sean transparentes, trazables y garanticen la igualdad de trato. Esto significa que **los proveedores de IA deben implementar medidas para evitar sesgos en los algoritmos que puedan conducir a discriminación** por razón de sexo, raza, nacionalidad, discapacidad u otras características personales protegidas.



La IA puede influir en la libertad de expresión, especialmente en contextos donde se utiliza para moderar contenido en plataformas digitales. El Reglamento aboga por un equilibrio entre la regulación de los sistemas de IA y la salvaguarda de la libertad de expresión, asegurando **que no se produzcan censuras indebidas ni se limite el discurso legítimo**.

El derecho a la explicación es un principio fundamental en el contexto de la IA, de modo que los usuarios y las personas afectadas por decisiones tomadas con el apoyo de sistemas de IA, **tienen derecho a ser informados sobre la lógica involucrada, el alcance y los efectos previstos** de dichos sistemas. El Reglamento requiere que los sistemas de IA ofrezcan un nivel adecuado de transparencia para que las personas puedan entender y, si es necesario, impugnar u oponerse a esas decisiones.

Como sucede en otras normas europeas, y en este caso con mayor motivo, el Reglamento incorpora, como parte esencial de su regulación, el enfoque a riesgos al cual ya he hecho referencia previamente, de modo que **establece obligaciones según el nivel de riesgo** que pueda suponer el sistema de IA.

Según lo anterior, el enfoque a riesgos del Reglamento Europeo de Inteligencia Artificial constituye uno de los pilares fundamentales de la regulación. Este enfoque se centra en la **identificación y clasificación de los sistemas de IA según el nivel de riesgo** que presentan para los derechos y libertades de las personas, así como para la seguridad y el bienestar general.

Resulta muy relevante constatar que en esta norma se identifican los sistemas que generan un **riesgo inaceptable,** que son aquellos que se consideran que constituyen una **clara amenaza para la seguridad, los medios de subsistencia y los derechos de las personas**. Estos sistemas **están prohibidos debido a su naturaleza intrínsecamente perjudicial o a su uso en contextos que pueden violar derechos fundamentales**, por ejemplo, el uso de IA para la manipulación de las personas o el control indiscriminado de la ciudadanía.

Es importante destacar que **la clasificación del riesgo que supone un sistema de IA puede cambiar a lo largo de su ciclo de vida** debido a modificaciones en su funcionamiento o uso, o incluso por modificaciones regulatorias. Por tanto, los proveedores deben realizar una **evaluación continua del nivel de riesgo** y cumplir con los requisitos reglamentarios correspondientes a la clasificación en que se encuentra el sistema de IA en cada momento.



Aunque me he referido de manera específica al Reglamento Europeo, no se puede obviar que la inteligencia artificial es una **preocupación a nivel mundial**, así que diversas regiones y países han desarrollado o están en proceso de elaborar marcos regulatorios y directrices para la gestión y el uso de la Inteligencia Artificial (IA). Estas iniciativas reflejan la importancia creciente de la IA y la necesidad de **abordar sus implicaciones éticas, sociales y económicas**; a continuación, se identifican algunas de las iniciativas más destacadas fuera del ámbito de la Unión Europea:

- En **Latinoamérica** la regulación de la IA está en una etapa incipiente. Algunos países han comenzado a explorar políticas públicas y marcos normativos para abordar los desafíos que plantea la IA, por ejemplo, en Brasil, México y Chile.
- En el **continente africano** se está comenzando a identificar la importancia de la IA para su desarrollo futuro, tenemos algunos ejemplos de ello en Ruanda y Sudáfrica.
- Podemos considerar que **Asia** es una región líder en el desarrollo y aplicación de la IA, con varios países estableciendo marcos regulatorios, como China y Singapur.
- En **Oceanía**, Australia es pionera en la regulación de la IA, ha publicado un marco ético para la IA, que incluye principios voluntarios para el diseño, desarrollo y aplicación de la IA.
- **Y en lo que respecta a Estados Unidos y Canadá** han tomado un enfoque más descentralizado y sectorial en la regulación de la IA, en los Estados Unidos varias agencias federales han desarrollado directrices para la IA en sectores específicos, como la salud, el transporte o la defensa, y en Canadá se han propuesto principios éticos para guiar el desarrollo de la IA.

Estas iniciativas internacionales reflejan un enfoque diverso en la regulación de la IA, con algunos países enfocándose en la promoción de la innovación y otros en la protección de los derechos éticos y sociales, por eso, **la cooperación internacional y el intercambio de mejores prácticas** serán esenciales para abordar los desafíos transfronterizos que presentará la IA.

08

Capítulo 8.

El uso ético de las TIC



Cuando se trata de abordar el uso ético de las TIC, lo que subyace es la aplicación de la ética empresarial de las organizaciones que desarrollan y comercializan soluciones tecnológicas, especialmente de las empresas dominantes del sector de las tecnologías de la información.

Lo cierto es que si bien los aspectos de la ética empresarial ya tiene un cierto recorrido, y existen numerosos trabajos al respecto, así como aplicaciones prácticas, no podemos considerar que su implantación este lo suficientemente extendida, dado que podemos encontrar **multitud de ejemplos en todos los sectores productivos en los que las empresas han actuado con absoluta falta de ética**, con los consecuentes efectos negativos, ya sean afectando al medioambiente, a las finanzas, a la seguridad alimentaria, a la competencia, o en general a los consumidores y usuarios de los servicios que se han visto afectados negativamente, por decisiones tomadas con una flagrante falta de ética empresarial.

De manera muy sintética, la "ética" es una disciplina de la filosofía que estudia *"el bien y el mal y sus relaciones con la moral y el comportamiento humano"*, es decir, estudia sobre qué fundamentar que "algo" sea bueno, o cómo discernir que algo sea moralmente correcto, por tanto, analiza los parámetros que permiten establecer lo que es correcto o incorrecto en un determinado contexto.

La ética influye en cómo son las normas. La ética tiene un componente de relatividad, ya que depende en buena medida de la sociedad y de la época, de modo que los valores y principios de cada sociedad y momento, pasan a convertirse en normas orientadas a limitar las conductas y a favorecer la convivencia, a priori, basándose en el respeto y la justicia, pero esa aplicación de la ética puede dar diferentes resultados, entre diferentes sociedades.

Por ejemplo, si una sociedad considera que el libre acceso a la información es un valor a proteger, o que la información es un bien público o social, se dotará de unas normas que faciliten ese acceso a la información, entre las que, por ejemplo, se incluya una concepción de los derechos de autor orientada a fomentar la actividad intelectual, y no a impedir el acceso a la información, o a dificultar la generación de conocimiento.

La ética de los negocios tiene que ver con implantar determinadas prácticas empresariales, que incluyen **normas y valores aceptados por la sociedad en la que la empresa desarrolla sus actividades**.

Cada vez más, los clientes y los ciudadanos esperan que las empresas se comporten de manera transparente, favoreciendo el desarrollo y asumiendo sus responsabilidades, y eso requiere de la **adopción de unos principios éticos por parte de las organizaciones**.

Por supuesto, las empresas también saben detectar los beneficios que eso les puede reportar en la gestión empresarial y en la mejora de cómo se les percibe externamente, es decir, como puede ganar valor su reputación empresarial; esa ética debe alcanzar a toda la organización, no se puede incorporar parcialmente.

Así en el ámbito de la denominada **"ética de la información"**, que vendría a abordar todo lo que tiene que ver con los usos aceptables e inaceptables de la información, se tienen en consideración cuestiones vinculadas, por ejemplo, a la propiedad intelectual, a la censura previa o a la integridad de la información, al uso de la información en el sector público, la confidencialidad de los datos personales, el respeto a la intimidad y al honor personal y familiar, el acceso a la información, los movimientos transfronterizos de datos, etc.

Desde el punto de vista empresarial la conjunción entre ética y legalidad se podría resumir en que **la organización debe motivar "intelectualmente" sus acciones en términos de ética y actuar materialmente en términos de legalidad**.

Un dilema que plantea el uso de las TIC es si realmente contribuye al desarrollo de la humanidad, en el sentido positivo, y si los usuarios hacen un uso responsable de los medios que tienen a su alcance, o bien al contrario, amplifica las conductas nocivas, o empuja a comportamientos moralmente incorrectos.

Por ejemplo, existen diversos estudios que hacen referencia al **consumo de energía y agua que implica el uso de la IA**, y en consecuencia sobre su impacto medioambiental[17], ya que una

[17] ¿Cuánta agua consume realmente la inteligencia artificial?

inocente consulta sobre cómo hacer una paella u otra receta, consume energía y agua, y no es tanto el consumo que hace esa consulta aislada, la cuestión es el volumen de consultas de ese tipo que se plantean cada pocos segundos a los diferentes asistentes de IA. Por supuesto, si se trata de generar imágenes o vídeos, el consumo crece exponencialmente, así la pregunta que debemos hacernos es si es ético pedirle a la IA que nos aconseje sobre qué ropa ponernos para un evento social, o que nos haga un vídeo de una pareja de gatos siameses bailando “rock and roll” en la playa.

La rápida evolución de las tecnologías y el crecimiento en su uso, así como la capacidad de las personas para adaptarse y asimilar esos cambios, en base a la construcción de nuevos valores, se han alineado, ya que los parámetros tradicionales de los que se infieren las conductas correctas e incorrectas han quedado más que superados, pasando a ser obsoletos, no solo desde el punto de vista ético, también normativo.

En el contexto de uso de la IA resulta especialmente relevante la aplicación de la ética, por eso el Reglamento Europeo de Inteligencia Artificial no solo aborda cuestiones de cumplimiento y regulación técnica, sino que también pone un énfasis significativo en los aspectos éticos de la IA.

La ética en la inteligencia artificial se refiere a los **principios y valores** que deben guiar el diseño, desarrollo, implementación y uso de sistemas de IA para asegurar que estos actúen en beneficio de la sociedad y respeten los derechos humanos.



La propia regulación europea propone una serie de principios éticos fundamentales que deben ser incorporados en todos los sistemas de IA, estos incluyen:

- **Respeto a la autonomía humana:** Los sistemas de IA deben permitir que los individuos tomen decisiones informadas y sean libres de tomar sus propias decisiones sin coacción o manipulación por parte de la IA.
- **Prevención de daños:** Se debe priorizar la seguridad y la integridad física y mental de las personas. Los sistemas de IA deben ser seguros y operar de manera que se minimice el riesgo de causar daño.
- **Justicia y equidad:** Los sistemas de IA deben ser diseñados y operados de manera que promuevan la justicia y la igualdad, evitando la discriminación y garantizando la equidad en el acceso y los resultados.
- **Transparencia y explicabilidad:** Debe ser posible entender y explicar las decisiones y procesos de los sistemas de IA. Esto es esencial para generar confianza y permitir la rendición de cuentas.

El Reglamento pretende establecer un marco en el **que la ética de la IA no sea una reflexión posterior**, sino una **consideración integral en todas las etapas del ciclo de vida de los sistemas de IA**.

09

Capítulo 9.

Conclusiones



Aunque en el propio informe ya se aportan una serie de reflexiones que en realidad no dejan de ser conclusiones, me ha parecido útil finalizar este documento con algunas constataciones y reflexiones finales.

Las tecnologías de la información y la comunicación **son un bien irrenunciable** para la humanidad, las necesitamos, y nos pueden ayudar a mitigar muchos de los efectos negativos que la propia humanidad ha generado y genera.

El uso de las tecnologías alcanza a cualquier ámbito, aportando en muchos casos extraordinarios beneficios, pero a la vez exponiendo a riesgos a las personas, desde muchas perspectivas, es decir, **nos exponen a daños individuales y colectivos de todo tipo**, que deben ser conocidos, analizados y convenientemente abordados, para reducirlos.

La ética y las leyes pueden actuar de manera coordinada, y ser muy eficaces para garantizar un uso adecuado de las TIC, que sea leal y positivo para todos, pero no son la solución total, **ese uso adecuado también está en manos y en la voluntad de las personas**, a fin de que las tecnologías nos aporten más beneficios que perjuicios. La cultura y la educación en el uso de las tecnologías es imprescindible.

Aunque existen, en prácticamente todos los países, marcos jurídicos que regulan el uso de las tecnologías, si bien con diferente grado de desarrollo e implementación, **es urgente que el legislador aprenda a hacer leyes que regulen una realidad cambiante y en continua evolución**, los mecanismos legislativos tradicionales son incapaces de regular las nuevas realidades tecnológicas, por tanto, deben articularse nuevas formas de regular, que estén más adaptadas y sean más eficaces, y que permitan regular sociedades altamente tecnificadas y conectadas, sin dejar atrás a aquellos que tienen menos opciones o posibilidades a usar o aprovechar las tecnologías.

Los humanos debemos gobernar las tecnologías, no nos podemos permitir el lujo de que las tecnologías gobiernen a la humanidad, **es inaceptable que los algoritmos definan lo que está bien y lo que está mal para los humanos** y menos aún que los algoritmos no estén sujetos a ningún control.

Y, finalmente, todo suma, y como señalaba en el prólogo, si todos y cada uno de nosotros somos un grano de arena, entre todos acabaremos siendo parte de algo mucho más grande.



BIBLIOGRAFÍA

1. **Jefatura del Estado (España). (2010, 17 de septiembre).** Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE-A-2010-14221). Boletín Oficial del Estado, (226), 79226–79253.
2. **OBS Business School. (2025).** Informe OBS: España y su normativa de ciberseguridad.
3. **OBS Business School. (2024).** Informe OBS: Estado de la Ciber-Inseguridad.
4. **FayerWayer. (2023).** Inteligencia Artificial: La historia de Michihito, el robot que estuvo a punto de ser alcalde de una ciudad en Japón.
5. **Harvard Law School.** (s. f.). Lawrence Lessig.
6. **Interactivity. (2024).** ¿Está el 57% de Internet creado por IA? Agencia de Marketing Online.
7. **Lessig, L. (1998).** The laws of cyberspace. Harvard Law School.
8. **Marketing4eCommerce. (2026).** El 90% del contenido de internet en 2026 será generado por inteligencia artificial.
9. **Redacción Digital Trends Español. (2026).** La internet muerta es realidad: el 17% de internet es generada por IA. Digital Trends Español.
10. **Stanford Institute for Human-Centered Artificial Intelligence. (2026).** The 2026 AI Index Report. Stanford University.

OBS Business School

www.obsbusiness.school

RED DE EDUCACIÓN SUPERIOR

Planeta Formación y Universidades