uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: **-Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

TEMA 1: TECNOLOGÍA Y DERECHO DIGITAL

II. Las Tecnologías de la Información y su incidencia en el derecho

Elaborado por PhD. Mª NIEVES DE LA SERNA BILBAO
Profesora Titular de Derecho Administrativo// Departamento de Derecho Público
Codirectora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid

SUMARIO:

II.- Las Tecnologías de la Información y su incidencia en el derecho

1.- Aspectos positivos y negativos de las TIC

Como ya se ha expuesto la incorporación de la tecnología ofrece importantes oportunidades en todas las áreas de la sociedad –en la educación, en la salud, en la agricultura, en la ganadería, en el medio ambiente, en los procesos industriales y productivos e incluso en lo que se conoce como gobernanza pública, entre muchos otros-. Se trata de una importante innovación que cuyo uso es demandado por todos los sujetos para incorporarla a sus actividades para así poder obtener todos los beneficios que la misma les reporta. El conjunto de la sociedad demanda tecnología para innovar y mejorar la productividad, para acceder al conocimiento, relacionarse y comunicarse, para ofrecer servicios, obtener formación, mejorar la salud, etc.. Por su parte, los poderes públicos también demandan estas tecnologías y las incorporan en sus actividades, pero también les corresponde prestar atención a este fenómeno para analizar y abordar los distintos retos jurídicos que las mismas conllevan. Es necesario, por tanto, contar con una sociedad preparada para afrontar todas las ventajas y problemas que las distintas tecnologías y sus avances puedan plantear.

En este contexto, la Unión Europea se ha comprometido a facilitar el avance científico, preservar el liderazgo tecnológico y garantizar que los avances tecnológicos estén al servicio de todos los europeos (tanto sujetos privados como públicos), de manera que se utilicen para mejorar sus vidas al mismo tiempo que respeten los principios y los derechos[1]. Por ello, se apuesta por

[1] Comisión Europea. Libro Blanco sobre Inteligencia Artificial (2020) https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

identificar las cuestiones jurídicas y éticas esenciales que plantea la tecnología para establecer un marco regulatorio adecuado.

Los retos que plantean el uso masivo de las nuevas tecnologías son variados. Por ejemplo, cuando se utiliza tecnología se va dejando lo que se denomina "huellas de información digitales", a través de las cuales se genera una multitud de datos, no sólo a nivel local sino, también, a nivel global. Así, cuando se compra un billete de avión, se crea una red social, se participa en ella, se paga con la tarjeta de crédito o móvil, se compra por internet, se utiliza el teléfono, etc., se dejan huellas de información. Estas huellas se guardan, utilizan, tratan, intercambian y almacenan generando importantes oportunidades de negocio[2]. Para tener una idea, basta mencionar como ejemplo que la recogida e intercambio de información se ha incrementado de manera exponencial en los últimos tiempos a tal punto que en cinco años –2015 a 2020- la información procesada se multiplicó por diez; en el año 2015, se generaron 80 *exabytes*[3] de datos y cinco años después, 800 *exabytes*. Este camino de recolección continuará ascendiendo. Tanto es así, que la generación de aquella información, su recogida, tratamiento, intercambio y almacenamiento permitió la aparición de fenómenos bien conocidos como el Big Data o el Cloud Computing que el Derecho ha debido abordar. En este sentido cabe mencionar la aprobación, en 2015, de la Recomendación UIT_T Y.3600 "Grandes volúmenes de datos-requisitos y capacidades basados en la computación en la nube" elaborada por la Unión Internacional de Telecomunicaciones (organismo dependiente de la ONU). En esta recomendación se utiliza una terminología común, describe el significado de los Big Data y las características del ecosistema de los Big Data desde la perspectiva de la normalización. Igualmente se señala cómo aprovechar los sistemas de computación en la

[2] Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation*, *28*, S22-S29. Disponible en: https://www.sciencedirect.com/science/article/pii/S1742287619300222

[3] Unidad de medida de la capacidad de memoria o del tamaño de los datos equivalente a 1024 petabytes (2 60 bytes). Real Academia Española y Asociación de Academias de la Lengua Española (2023). «exabytes». *Diccionario panhispánico de dudas* (2.ª edición, versión provisional).

nube para ofrecer servicios de Big Data y cómo ayudar a la industria para la gestión de grandes conjuntos de datos imposibles de transferir y analizar utilizando tecnologías tradicionales de gestión de dato[4].

También se ha pronunciado al respecto la Unión Europea. En el paquete de medidas adoptada sobre protección de datos en 2016, persigue que Europa esté preparada para afrontar la era digital. Todos los europeos deben tener el mismo derecho a la protección de sus datos con independencia del lugar donde se realice su tratamiento[5].

No obstante, no podemos dejar de mencionar que a pesar de los esfuerzos por regular la tecnología para proteger los derechos de las personas; su utilización sigue suponiendo riesgos, incertidumbres, desconfianza, peligros que deben ser detectados y abordados con rapidez para evitar que se produzcan efectos no deseados que, en algunos casos, pueden llegar a tener consecuencias irreversibles para las personas. Ejemplo de ello son las intromisiones en la intimidad tales como el *cyberbullying*, los robos de información o la publicación de datos íntimos personales, por citar algunos. Corresponde, por tanto, al Derecho, acometer la tarea de proteger y limitar los riesgos ofreciendo garantías y velando por la seguridad a la que luego nos referiremos.

Todo uso de la tecnología debe ser fiable y ofrecer confianza y eso sólo se puede conseguir, como señala la Unión Europea, si existe un marco estratégico basado en los derechos humanos y valores fundamentales, que anime, al mismo tiempo, a las empresas, a los poderes públicos y a las personas a desarrollarlas. Es, por tanto, tarea de los poderes públicos y de la sociedad emprender un debate riguroso y tranquilo sobre las consecuencias que

[4] Consultar en el siguiente enlace: https://www.itu.int/rec/T-REC-Y.3600-201511-I/es
[5] Nos referimos especialmente al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) ELI: http://data.europa.eu/eli/reg/2016/679/oj

conlleva el uso de esta tecnología, las innovaciones que aporta y los riesgos que conlleva[6]

Otro gran reto en el uso de la tecnología es en materia de seguridad. Se suele decir, que la seguridad es un concepto asociado a la ausencia de riesgo, pero en la tecnología y en las redes no resulta posible garantizar que aquel desaparezca totalmente. El elemento de riesgo siempre está presente con independencia de las diversas medidas que se puedan adoptar para limitar el riesgo. Los expertos suelen indicar que no existe un sistema de seguridad absoluto, existen niveles de seguridad, que se definen, con carácter general, como un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en las redes y sistemas para proteger la información[7]. El Derecho no ha sido ajeno a esta materia a pesar de ser muy técnica. A nivel europeo se han aprobado diversas normas entre las que cabe mencionar la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (Security of Network and Information Systems)». En España, esta norma se transpuso por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y por su norma de desarrollo, el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. No obstante, recientemente entro en vigor la La Directiva (UE) 2022/2555, conocida como NIS2, establece

[6] Comisión Europea. Libro Blanco sobre Inteligencia Artificial (2020) https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

[7] Como artículo de interés se puede consultar: FASLI, M. (2007). On agent technology for e-commerce: trust, security and legal issues. *The Knowledge Engineering Review*, *22*(1), 3-35. Disponible en: https://www.cambridge.org/core/journals/knowledge-engineering-review/article/abs/on-agent-technology-for-ecommerce-trust-security-and-legal-issues/BAFFE67541CD87091C60E28AF995D6C1

principalmente obligaciones de ciberseguridad para los Estados miembros y medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación[8]. En primer lugar, la Directiva NIS2 establece las obligaciones de los Estados miembros en las siguientes materias: preparación, mantenimiento y difusión a la Comisión de una lista de entidades significativas y esenciales; adopción de la estrategia nacional de ciberseguridad, información proporcionada por la Comisión y evaluación periódica; designar agencias responsables de ciberseguridad, regulatorias y de punto único e informar y proporcionar recursos a los comités para llevar a cabo sus funciones; desarrolla un plan nacional de gestión de crisis de ciberseguridad y selecciona autoridades competentes y determina capacidades; significa el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y proporciona recursos, capacidades técnicas y colaboración efectiva; nombrar un CSIRT para coordinar la divulgación de vulnerabilidades; garantizar la cooperación a nivel nacional (así como normas de cooperación a nivel europeo); y con respecto al seguimiento y la aplicación, garantizar que las autoridades competentes realicen un seguimiento efectivo y adopten las medidas necesarias, incluidos sistemas de sanciones.

En segundo lugar, la Directiva NIS2 impone las siguientes obligaciones a las entidades dentro de su alcance (como se establece en los Anexos 1 y 2), que se resumen a continuación: adoptar medidas de gobernanza, gestión de riesgos de ciberseguridad e información (informes); adoptar medidas técnicas y organizativas adecuadas para la gestión de los riesgos de ciberseguridad; y prevenir y reducir el impacto de posibles incidentes cibernéticos; notificar al CSIRT o a las autoridades pertinentes sobre incidentes de seguridad cibernética; los gerentes reciben capacitación sobre riesgos de ciberseguridad y son responsables de tomar las acciones apropiadas; utilizar el esquema de certificación europeo; envía la información necesaria a la autoridad competente

[8] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). ELI: http://data.europa.eu/eli/dir/2022/2555/oj

y notifica los cambios en la misma. También se considera el intercambio voluntario de información de seguridad cibernética entre entidades esenciales y críticas y la notificación voluntaria a las autoridades o al Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de todos los incidentes, amenazas cibernéticas o cuasi accidentes relacionados.

La directiva NIS 2 amplía su alcance a una serie de entidades medianas y grandes en sectores que son importantes para la economía y la sociedad, incluidas las comunicaciones electrónicas, los servicios digitales, la gestión de aguas residuales y residuos, la fabricación de productos esenciales y los proveedores de servicios postales y urgentes nacionales. y administraciones nacionales. (Para España, unidades administrativas generales; unidades administrativas nacionales en las comunidades autónomas; el ámbito de aplicación podrá ser determinado por las unidades administrativas públicas de nivel local). Otras mejoras significativas en la directiva NIS 2 incluyen que tiene en cuenta la seguridad de las cadenas de suministro y las relaciones con los proveedores; introduce la responsabilidad de la alta dirección por las fallas de seguridad cibernética.

Desde un punto de vista nacional cabe destacar la reciente aprobación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que deroga al Real Decreto 3/2010, de 8 de enero, por el que se regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Este nuevo Esquema Nacional, tal como señala el artículo 1, determina los principios básicos y los requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por el sector público, con el fin de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. Al igual que el anterior Real Decreto, el mismo también será un referente en el ámbito privado y de manera particular para las empresas que tienen relación vigente con las

administraciones y empresas públicas y para todas aquellas que quieran contratar con ellas[9].

Corresponde, por tanto, sopesar, estudiar, analizar y valorar desde todos los puntos de vista los aspectos positivos y negativos que las tecnologías ofrecen y, sin renunciar a su implementación para obtener los máximos beneficios, el Derecho debe abordar su implementación y uso, limitar los beneficios, así como atajar y minimizar los efectos negativos. En toda esta tarea el Derecho resulta una herramienta crucial, necesaria e imprescindible.

2. Relación entre Derecho e innovación

Como se ha apuntado, al abordar la Unión Europea la incorporación de la tecnología a nuestras vidas apuesta por un enfoque basado en la regulación. Pero también es consciente de que para que el Derecho pueda regular el uso de la tecnología no puede seguir acudiendo a instituciones tradicionales. La tecnología cambia e innova constantemente y por tanto el derecho precisa actualizarse, transformarse, adaptarse al ritmo de los cambios de aquella.

[9] En relación con la ciberseguridad se debe tener presente la función encomendada al Centro Criptológico Nacional (organismo adscrito al Centro Nacional de Inteligencia) Su principal objetivo es facilitar y coordinar la respuesta a incidentes de forma rápida y eficiente en una red de organizaciones del sector público. Este último detalle sobre la organización pública es importante en este caso, ya que será la principal diferencia con INCIBE. Este último está dirigido a entidades privadas, mientras que CCN-CERT se centra en el sector público. Además de dar respuesta a las incidencias, también tiene otras tareas importantes, como la de regulador de la ENS (Iniciativa Nacional de Seguridad) o la creación y distribución de herramientas de ciberseguridad, de las que hablaremos ahora. Por otra parte, el Instituto Nacional de Ciberseguridad (INCIBE), anteriormente Instituto Nacional de Tecnologías de las Comunicaciones (INTECO), es una empresa de dependiente de la Consejera de Digitalización e Inteligencia Artificial del Ministerio de y Transformación Digital y actúa como unidad de referencia para el desarrollo de ciudadanos, redes académicas y de investigación de Ciberseguridad y Confianza Digital, profesionales, empresas y sectores especialmente estratégicos. Es importante destacar que INCIBE depende en gran medida de los ciudadanos finales. Esto significa que lleva a cabo una serie de actividades para concienciar, educar y proteger a los ciudadanos comunes y corrientes. Además, promocionar D i y atraer profesionales. Es importante saber que INCIBE pone a disposición de todas los ciudadanos (incluidos menores) y empresas un número de teléfono confidencial y gratuito a nivel nacional para todas las incidencias de ciberseguridad 017. (https://www.incibe.es/linea-de-ayuda-en-ciberseguridad)

Resulta necesario, pues, perfilar las relaciones entre el Derecho y la innovación de tal forma que la sociedad pueda aprovechar las oportunidades que la tecnología le ofrece para mejorar la vida pero, también, para protegerla, eliminando, atajando o minimizando, en la medida de lo posible, los efectos negativos que aquellas ocasionan. Ahora bien, para conseguir este objetivo el Derecho debe afrontar nuevos retos. Como destaca el profesor Parejo Alfonso, estamos inmersos en un sistema en el que el Derecho se encuentra en un continuo proceso de transformación[10]. Nuestra sociedad es compleja, contradictoria e innovadora a la que le es inherente la incertidumbre y el riesgo. Ante aquel panorama es difícil vislumbrar el sistema que se está fraguando. No obstante, para el autor citado, si bien el Derecho continúa generando orden, el mismo se consigue a través de *"los requerimientos innovadores de la dinámica social actual (el credo de la "modernización continua")*", al que se exige una estrategia simultánea que permita la innovación y la resolución de los problemas que de aquella derivan. En particular, señala, se reclama la presencia del Derecho para que ofrezca seguridad frente a los peligros y los riesgos que la evolución científico técnica trae, de tal forma que cuanto mayor es el riesgo o el peligro que se percibe de aquella evolución, mayor es la demanda al Derecho. De ahí que Parejo Alfonso concluya que el mayor reto para el Derecho frente a la innovación es mantener las innovaciones dentro de unos límites aceptables demandados por la sociedad, es decir, que garantice el respeto a unos valores y fines sociales, constitucionales, de tal forma que se puedan aprovechar las ventajas que ofrece la innovación pero, se neutralicen en lo posible, los riesgos que aquella pueda traer (así por ejemplo aunque se demande que la inteligencia artificial sea utilizada para mejorar prestaciones y servicios, a la vez se exige que el Derecho nos proteja de los peligros, riesgos y consecuencias que su uso pueda ocasionar).

Sea como sea, el Derecho clásico no puede ser impermeable ante la innovación. Su articulación se presenta inadecuada para afrontar el reto que

[10] PAREJO ALFONSO, L.; (2018) Lecciones de Derecho Administrativo, edit Tirant Lo Blanch, Valencia, págs.,70 y ss.

suponen las tecnologías y su incorporación a nuestras vidas. Las innovaciones resultan imparables y su introducción desplaza a la aplicación del Derecho. Ahora bien, el Derecho no puede desaparecer, su utilidad y su exigencia es incuestionable, en particular, para concretar valores y principios, afrontar la prevención de riesgos, concretar límites, eliminar cualquier efectos perjudicial, etc.. No obstante, para que así sea, su presencia y eficacia requiere de cambios importantes. Algunos mecanismos potenciados por este nuevo escenario son, entre otros, la renuncia a la regulación a favor del establecimiento de la autorregulación que viene fundamentalmente a limitar la existencia de normas imperativas, de cuño unilateral; o la corregulación o regulación híbrida en la que participa el poder público, la representación civil de la sociedad y el sector empresarial o las asociaciones privadas que garantizan a través de la certificación el cumplimiento de estándares públicos. Algunos de ellos luego abordaremos con más detalle su estudio.

En definitiva, en palabras del profesor Parejo Alfonso *"el Siglo XXI precisa un Derecho siquiera parcialmente nuevo, que –en el movimiento actual de devolución de responsabilidad a la sociedad que expresa en el Estado garante- debe evitar caer en el exceso, como alerta ya el hecho de que cuando se precisa la defensa frente a peligros o la compensación de perjuicios también los que consideran al Estado como un mal, claman por su intervención. El Estado conserva intacta, en efecto, su responsabilidad política y jurídica por el interés común. Y justamente por ello está obligado a reconvertir su instrumentario de acción; reconversión en la que indefectiblemente viejo y nuevo Derecho se mezclan no siempre con la conveniente coordinación*"[11].

2.1 Legal Tech; la innovación jurídica

[11] Ob.cit; pág 73

A. Definición y Ámbito del Legal Tech

En los últimos años, la intersección entre la tecnología y el derecho ha transformado radicalmente la manera en que los servicios legales son prestados. Un fenómeno nuevo en este ámbito es el conocido como "Legal Tech", término que abarca una amplia gama de tecnologías diseñadas para mejorar la eficiencia, la accesibilidad y la calidad del servicio en el ámbito jurídico. Desde plataformas que automatizan procesos básicos hasta herramientas avanzadas basadas en inteligencia artificial (IA), Legal Tech está alterando los paradigmas tradicionales del ejercicio legal y plantea desafíos y oportunidades significativas para los abogados, las firmas y el sistema de justicia en su conjunto.

El término Legal Tech se refiere a la utilización de tecnologías digitales para prestar o mejorar servicios legales. Esto incluye software para la gestión de despachos, plataformas para la automatización de contratos, herramientas de análisis legal basadas en IA, sistemas de resolución de conflictos en línea, entre otros. Las aplicaciones de Legal Tech no solo están dirigidas a abogados sino también, a clientes, a jueces y a partes interesadas en el proceso legal. Su alcance es extenso y permite desde el manejo de documentos, la gestión de casos hasta la previsión de resultados legales basados en datos históricos.

Un ejemplo común de Legal Tech es el uso de plataformas de automatización de documentos que permiten a los abogados generar contratos y otros documentos legales de forma más rápida y precisa. Se trata de herramientas que han reducido el tiempo que los despachos o profesionales dedican a tareas repetitivas y administrativas y que permiten a las firmas legales concentrarse más en aspectos estratégicos y sustantivos del trabajo jurídico.

B. Beneficios del Legal Tech

Uno de los principales beneficios de Legal Tech es el aumento de la eficiencia, al permitir reducir el tiempo y los costos asociados con la prestación de servicios legales. En lugar de dedicar horas a la revisión manual de documentos o a la investigación legal, los abogados pueden utilizar herramientas de búsqueda avanzadas, análisis de datos y/o automatización para completar tareas en una fracción del tiempo limitada así como compartir documentos entre las distintas partes implicadas, redactar propuestas de documentos, etc.. Este aumento en la eficiencia se traduce en costos más bajos, en un servicio más accesible, participativo, dinámico y sin pérdidas de documentos, entre otros.

Además, Legal Tech facilita el acceso a la justicia. La tecnología puede reducir las barreras geográficas, permitiendo que los servicios legales sean accesibles para personas en áreas rurales o de bajos ingresos. Así, por ejemplo, plataformas en línea permiten a los clientes obtener asesoramiento jurídico o resolver disputas sin tener que visitar una oficina física. En un contexto en el que el acceso a la justicia ha sido un problema persistente, especialmente en regiones con recursos limitados, Legal Tech tiene el potencial de democratizar los servicios legales.

Otro beneficio clave de esta nueva tecnología es la mejora de la precisión y la reducción de errores humanos. En efecto, las herramientas basadas en inteligencia artificial pueden revisar contratos o realizar análisis legales más detallados y rápidos que los humanos, minimizando los errores en la redacción de documentos o en la interpretación de normativas complejas. Asimismo, la tecnología blockchain ofrece garantías en la seguridad de los registros y transacciones legales, lo que puede transformar sectores como la propiedad intelectual y la protección de derechos digitales.

C. Desafíos y Problemas Éticos del Legal Tech

A pesar de los numerosos beneficios, Legal Tech también plantea una serie de desafíos, particularmente en relación con la ética, la privacidad y la regulación.

Uno de los principales problemas es la calidad y seguridad de los algoritmos utilizados en las herramientas de Legal Tech. Los sistemas de IA, por ejemplo, pueden basarse en conjuntos de datos sesgados, lo que puede llevar a decisiones legales injustas o incorrectas. La falta de transparencia en el funcionamiento de estos algoritmos plantea preguntas sobre la rendición de cuentas y la responsabilidad cuando algo sale mal.

Asimismo, la adopción de Legal Tech podría aumentar la desigualdad entre quienes tienen acceso a estas tecnologías y quienes no. Mientras que las grandes firmas de abogados pueden permitirse implementar sistemas avanzados de automatización y análisis de datos, las firmas más pequeñas y los abogados independientes pueden enfrentar dificultades para mantenerse al día con las innovaciones tecnológicas, lo que podría generar una disparidad en la calidad del servicio prestado.

Otro desafío clave es la regulación de Legal Tech. A medida que la tecnología avanza más rápido que la legislación, los marcos regulatorios pueden quedarse atrás. Existen preocupaciones sobre la protección de datos y la privacidad en el uso de plataformas en la nube o en herramientas de IA, especialmente cuando se manejan datos sensibles de los clientes. Es necesario que los legisladores trabajen en la creación de normas específicas para abordar estos temas y garantizar que el uso de la tecnología en el ámbito jurídico no comprometa los derechos fundamentales de las personas.

D. El Futuro del Legal Tech

El futuro de Legal Tech parece prometedor, con un crecimiento exponencial en el desarrollo de nuevas herramientas y plataformas diseñadas para revolucionar el sector legal. Las tendencias actuales indican que tecnologías como la inteligencia artificial, el aprendizaje automático, el blockchain y los smart contracts continuarán desempeñando un papel crucial en la transformación de la práctica jurídica. Se espera que la automatización siga

avanzando, eliminando tareas tediosas y repetitivas de los abogados, permitiéndoles enfocarse en aspectos estratégicos del trabajo. Además, el Legal Te4h podría generar un cambio en el modelo de negocio tradicional de las firmas de abogados, con una mayor orientación hacia soluciones tecnológicas innovadoras, lo que podría cambiar la dinámica de precios y la estructura del mercado de servicios legales. Sin embargo, para que Legal Tech alcance su máximo potencial, será necesario un esfuerzo conjunto de abogados, tecnólogos y reguladores. La adopción de estas tecnologías debe ser acompañada de una comprensión profunda de sus implicaciones legales, éticas y sociales. Asimismo, los abogados deberán adquirir nuevas habilidades tecnológicas para no quedar rezagados en un mundo cada vez más digitalizado.

En definitiva, Legal Tech representa una oportunidad sin precedentes para transformar la práctica del derecho, haciéndola más eficiente, accesible y precisa. Sin embargo, también plantea desafíos éticos, regulatorios y de seguridad que no deben ser ignorados. El éxito de esta transformación dependerá de un equilibrio entre la innovación tecnológica y la protección de los principios fundamentales del derecho, asegurando que la tecnología sirva para mejorar, y no para comprometer, el acceso a la justicia y la equidad en los sistemas legales.

3 Modelos complementarios como soluciones sustitutivas de los enfoques tradicionales legislativos vigentes en el mundo digitalizado

3.1 Corregulación y Autorregulación

Como ha quedado expuesto resulta indudable que en esta nueva era digital la forma de abordar la regulación de los sectores afectados por la tecnología supone acometer cambios con el fin de adaptarse al ritmo de la innovación tecnológica. Los modelos tradicionales de relación y de organización política ya no sirven y cuestiones como la seguridad nacional, la información, la sociedad hiperconectada, la inteligencia artificial, la sociedad de los datos, etc, deben ser abordados de manera distinta y corresponde al Derecho defender el interés general. Es por ello que el Derecho debe promover la innovación tecnológica sin limitarla, pero para ello es necesario repensar la clásica función de legislar para concretar un marco de convivencia social en el que el Derecho y la innovación tecnológica compartan objetivos, definan valores y fines, señalen limitaciones, etc.. Se debe, por tanto, asumir cambios en la técnica regulatoria clásica de tal forma que se adapte a los requerimientos innovadores de la dinámica social actual. En cualquier caso, el Derecho debe seguir existiendo y asumir un papel destacado pero su ritmo de producción debe adaptarse a la modernización continua. En este sentido, las instancias europeas vienen fomentando la participación de los sujetos implicados para garantizar la efectividad del Derecho, habilitando modelos complementarios como soluciones sustitutivas de los enfoques tradicionales legislativos vigentes en este mundo digitalizado. Se trata de la corregulación y autorregulación, instrumentos que suelen estar autorizados y promocionados por la propia normativa eliminando de manera directa las normas de tipo imperativo.

En el ámbito europeo, según el sector o el problema abordado, la normativa fomenta el uso de otras técnicas regulatorias que completan la regulación existente para que la misma tenga una mayor efectividad. Aquella técnica se materializa bien, a través de la adopción de pactos entre los poderes públicos y los propios actores afectados, técnica conocida con la denominación de corregulación o regulación híbrida, bien, a través de la delegación por parte de la norma en los propios sujetos o sectores afectados para la concreción definitiva de la regulación para su sector concreto, técnica conocida como autorregulación.

Tanto la corregulación, como la autorregulación forman parte, junto con la regulación existente, de los mecanismos de ordenación de un determinado sector de actividad. En todo caso, baste señalar que, dependiendo de las tradiciones jurídicas de cada lugar, ambos sistemas se suelen utilizar como complemento de los mecanismos legislativos vigentes en tanto que constituyen una valiosa contribución a la consecución de los objetivos de la normativa correspondiente.

Se trata de dos sistemas que cada día adquieren mayor protagonismo. En primer lugar, es preciso señalar que corresponde al legislador concretar qué planteamiento regulador es el más adecuado en cada caso. Es decir, es éste quien debe valorar si el sector objeto de regulación requiere una respuesta legislativa completa o si es posible utilizar otras alternativas complementarias que se adapten mejor a los cambios como los mecanismos de corregulación o la autorregulación, o ambos a la vez.

Tanto la corregulación como la autorregulación han demostrado, en distintas experiencias, su indudable utilidad. Se trata de sistemas que permiten en determinados sectores dotarse de normas más ajustadas a las exigencias del desarrollo específico de su actividad y que el legislador no puede conocer. Ambos sistemas han demostrado que, a través de los mismos los sujetos o sectores implicados se sienten más vinculados y propensos a cumplir con las normas establecidas en las que ellos han participado al aportar más claridad, ajuste con la actividad regulada y mecanismos de resolución alternativa de conflictos más reales, que propician, a la vez, una solución ágil y eficiente en las distintas controversias que puedan surgir.

En relación con cada uno de ellos, señalar que en la corregulación la función regulatoria se reparte entre las partes interesadas y el gobierno o, en su caso, las autoridades u organismos reguladores nacionales. Es así que, la propia norma habilita y fomenta para que las autoridades públicas correspondientes participen junto con los sujetos implicados en la concreción definitiva de la normativa aplicable al sector. Se trata de complementar los principios y criterios

recogidos en la normativa a través de la concreción de aquella a la actividad regulada. Suele ser común que en este tipo de normas de corregulación, los poderes públicos además de ser copartícipe en la elaboración definitiva de las normas aplicables al sector se reserven la posibilidad de vigilar o intervenir en caso de que no se cumplan los objetivos señalados en la norma aprobada fruto de un proceso de corregulación. Así, por ejemplo, en España esta labor se ha encomendado en algunos sectores, como en audiovisual, a la Comisión Nacional de Mercados y Competencia (conocida por las siglas CNMC)[12].

Respecto de la autorregulación, a diferencia del sistema anterior, las reglas son elaboradas por los propios actores, sin intervención alguna del poder público. Estos son los que determinan las bases, las limitaciones, el alcance, los compromisos y también los controles respecto del cumplimiento de lo dispuesto en la norma autorregulatoria. Estas normas, al igual que las anteriores, completan la regulación vigente y concretan de manera más específica pautas comunes de actuación para un determinado ámbito de actuación por lo que desarrolla las peculiaridades concretas del sector. De este modo, e señalan, de manera específica, la(s) forma(s) de cumplir con las obligaciones y los derechos, los procedimientos de reclamación o sanciones u organismos autorizados para intervenir en todos los procedimientos, incluido, los incumplimientos. En general, se trata de compromisos voluntarios en el que las partes afectadas por una norma se autorregulan en ámbitos específicos para lograr que exista una aplicación efectiva de aquella de acuerdo con las

[12] De conformidad con el apartado 5 del artículo 9 de la Ley 3/2013, de 4 de junio, de creación de la CNMC *"La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento del mercado de comunicación audiovisual. En particular, ejercerá las siguientes funciones: [...] 5. Velar por el cumplimiento de los códigos de autorregulación sobre contenidos audiovisuales verificando su conformidad con la normativa vigente, en los términos establecidos en el artículo 12 de la Ley 7/2010, de 31 de marzo"*. Por su parte, el artículo 12 de la LGCA relativo al derecho a la autorregulación del prestador del servicio de comunicación audiovisual, establece en sus apartados segundo y tercero que: *"2. Cuando un prestador apruebe un código por sí solo, o bien en colaboración con otros prestadores, o se adhiera a un código ya existente, deberá comunicarlo tanto a las autoridades audiovisuales competentes como al organismo de representación y consulta de los consumidores que correspondan en función del ámbito territorial de que se trate. Para los prestadores de ámbito estatal, dicho órgano es el Consejo de Consumidores y Usuarios. La autoridad audiovisual verificará la conformidad con la normativa vigente y de no haber contradicciones dispondrá su publicación*." Más información: https://www.cnmc.es/ambitos-de-actuacion/audiovisual#funciones

características específicas de la actividad o tareas propias de un sector concreto. Su aplicación no requiere, necesariamente, para su aplicación, de la existencia de un acto legislativo pero cada vez es más usual que las propias normas fomenten la autorregulación del propio sector.

3.2 Ejemplos de corregulación y autorregulación

No es posible estudiar o analizar todos los supuestos existentes de fomento y/o habilitación de este tipo de técnicas legislativas complementarias. Tan sólo cabe mencionar los denominados Códigos de conducta en materia de protección de datos, que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, «RGPD»), incita a las asociaciones u otros organismos a elaborar estos códigos dentro de los límites fijados por el propio reglamento, con el fin de facilitar la aplicación efectiva del mismo teniendo en cuenta las características específicas del tratamiento de datos llevado a cabo en determinados sectores y las necesidades específicas de las empresas[13].

EL RGPD concreta que cuando se vaya a: *«…elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas»*[14].

Igualmente señala en el artículo 40 que: *«Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del*

[13] Considerando 98 del RGPD
[14] Considerando 99 del RGPD

presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas»[15]

Finalmente, el Comité Europeo de Protección de Datos aprobó unas Directrices, concretamente, las Directrices 1/2019, del Comité Europeo de Protección de Datos, sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679, en las que señala que los códigos son: *«un método práctico, potencialmente rentable y valioso para lograr niveles superiores de coherencia de la protección para los derechos de protección de datos. Dichos códigos pueden actuar como un mecanismo que demuestre el cumplimiento del RGPD. Concretamente, pueden contribuir a eliminar las lagunas de armonización que puedan existir entre los Estados miembros en la aplicación de la legislación en materia de protección de datos. Asimismo, brindan la oportunidad a sectores concretos de reflexionar acerca de las actividades comunes de tratamiento de datos y acordar normas de protección de datos adaptadas y prácticas, que satisfagan las necesidades del sector y cumplan los requisitos del RGPD».*

Otro ejemplo importante de fomento de estas técnicas complementarias de corregulación y autorregulación adoptadas por la Unión Europea es el sector de comunicación audiovisual. La última Directiva aprobada, Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (en adelante, Directiva (UE) 2018/1808 de servicios de comunicación audiovisual), que se aplica tanto a los servicios lineales como a los servicios no lineales, fomenta aún más estos modelos complementarios de

[15] Considerando 98 y artículo 70, apartado 1, letra n), y los artículos 40 y 41 del RGPD y Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDPGDD. Art. 38 y disposición transitoria segunda.

regulación debido fundamentalmente a la evolución de las realidades del mercado. En dicha norma europea subraya lo siguiente:

«La experiencia ha demostrado que tanto los instrumentos de autorregulación como los de corregulación, aplicados de acuerdo con las distintas tradiciones jurídicas de los Estados miembros, pueden desempeñar un importante papel a la hora de otorgar un alto grado de protección a los consumidores. Las medidas para alcanzar los objetivos de interés general en el sector de los servicios emergentes de comunicación audiovisual resultarían más eficaces si se adoptan con el apoyo activo de los propios prestadores de servicios. La autorregulación constituye un tipo de iniciativa voluntaria que permite a los operadores económicos, interlocutores sociales, organizaciones no gubernamentales y asociaciones en general adoptar directrices entre sí y para sí. Son responsables del desarrollo de estas directrices, así como del seguimiento y aplicación de su cumplimiento. Los Estados miembros deben, con arreglo a sus respectivas tradiciones jurídicas, reconocer el cometido que puede desempeñar la autorregulación efectiva como complemento de los mecanismos legislativos, judiciales y administrativos vigentes y su valiosa contribución con vistas a la consecución de los objetivos de la Directiva 2010/13/UE. No obstante, si bien la autorregulación puede ser un método complementario para aplicar ciertas disposiciones .., en modo alguno puede sustituir a las obligaciones del poder legislativo nacional. La corregulación, en su mínima expresión, proporciona un «vínculo jurídico» entre la autorregulación y el poder legislativo nacional, con arreglo a las tradiciones jurídicas de los Estados miembros[16]»

Y el propio artículo 4 de la Directiva (UE) 2018/1808 de servicios de comunicación audiovisual , señala que:

[16] Considerandos 13 y ss. de la Directiva (UE) 2018/1808 de servicios de comunicación audiovisual

«1. Los Estados miembros animarán a que se use la corregulación y se promueva la autorregulación mediante códigos de conducta adoptados a nivel nacional en los ámbitos coordinados por la presente Directiva en la medida permitida por sus ordenamientos jurídicos. Dichos códigos deberán:

a) gozar de amplia aceptación entre los principales interesados en los Estados miembros de que se trate;
b) exponer de manera clara e inequívoca sus objetivos;
c) prever un seguimiento y evaluación periódicos, transparentes e independientes de la consecución de los objetivos perseguidos, y
d) prever los medios para una aplicación efectiva, incluidas unas sanciones efectivas y proporcionadas.

2. Los Estados miembros y la Comisión podrán fomentar la autorregulación mediante códigos de conducta de la Unión elaborados por los prestadores de servicios de comunicación, los prestadores de plataformas de intercambio de vídeos o las organizaciones que los representen, en cooperación, en caso necesario, con otros interesados como la industria, el comercio o las asociaciones u organizaciones profesionales o de consumidores. Dichos códigos deberán gozar de amplia aceptación entre los principales interesados en el ámbito de la Unión y cumplir lo dispuesto en el apartado 1, letras b) a d). Los códigos de conducta de la Unión se entenderán sin perjuicio de los códigos de conducta nacionales.

La Comisión, en cooperación con los Estados miembros, facilitará la elaboración de códigos de conducta de la Unión cuando proceda, de conformidad con los principios de subsidiariedad y proporcionalidad.

Los signatarios de los códigos de conducta de la Unión presentarán los proyectos de esos códigos y sus modificaciones a la Comisión. La Comisión consultará al Comité de contacto sobre dichos proyectos de códigos o modificaciones.

La Comisión pondrá los códigos de conducta de la Unión a disposición del público y podrá darles la publicidad adecuada

3. *Los Estados miembros seguirán teniendo la facultad de exigir a los prestadores de servicios de comunicación sujetos a su jurisdicción el cumplimiento de normas más detalladas o estrictas de conformidad con la presente Directiva y el Derecho de la Unión, en particular cuando sus autoridades u organismos reguladores nacionales independientes lleguen a la conclusión de que un código de conducta o partes del mismo han demostrado no ser suficientemente eficaces. Los Estados miembros comunicarán a la Comisión esas normas, sin dilaciones indebidas.».*

Siguiendo aquellos objetivos, la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual (si bien está pendiente de trasposición la Directiva (UE) 2018/1808 de servicios de comunicación audiovisual), fomenta estas técnicas al señalar, expresamente en el artículo 12, lo siguiente:

Los prestadores del servicio de comunicación audiovisual tienen derecho a aprobar códigos de autorregulación en los que se regulen los contenidos de la comunicación audiovisual y las reglas de diligencia profesional para su elaboración.

Es preciso destacar que, a partir de aquellas habilitaciones, en España se aprobaron en el ámbito de la comunicación audiovisual múltiples códigos de conductas, en particular, en el sector de la comunicación comercial, tarea principalmente desarrollada por un organismo independiente de autorregulación publicitaria, denominado Autocontrol. Se trata de una asociación, sin ánimo de lucro, integrada por anunciantes, agencias de publicidad, medios de comunicación y asociaciones profesionales que trabaja para que la actividad publicitaria sea leal, veraz, honesta y legal[17]. En el desarrollo de su función, Autocontrol ha trabajado y aprobado diversos Código, entre los que cabe destacar el Código Publicitario (1996) inspirado en el Código internacional de Prácticas Publicitarias de la Cámara de Comercio Internacional, el Código de Corregulación de la publicidad de alimentos y

[17] Véase al respecto la página web https://www.autocontrol.es/

bebidas dirigida a menores (2015); el Códigos de autorregulación de la Publicidad Infantil de juguetes, (2015), el Código de confianza Online (2019), o más recientemente, el Código de conducta de influencers (2020) o el Código sobre el tratamiento de datos en la actividad publicitaria en el ámbito digital (2020).

Resulta por tanto necesario revisar los escenarios regulatorios, así como las políticas públicas existentes e introducir estas nuevas formas de regulación de los sectores digitalizados, no sólo para cubrir posibles lagunas y fijar las condiciones básicas que permitan la transformación digital ordenada y eficiente, sino también para potenciar la innovación tecnológica, concretar obligaciones y garantizar los derechos y deberes de los ciudadanos. Para conseguir este objetivo resulta esencial que exista un compromiso estable de cooperación de todas las partes implicadas, es decir, del sector público, del sector privado y de la sociedad civil de tal forma que se pueda alcanzar una regulación válida, eficaz, útil y segura.