Eduardo Valpuesta Gastaminza / Juan Carlos Hernández Peña (Coords.). *Tratado de Derecho Digital.* La Ley-Wolters Kluwer, Las Rozas (Madrid), 2021, 880 pp.

Carlos Llorente Gómez de Segura
Abogado, Profesor de Universidad

DOI: 10.20318/CDT.2022.7260

1. Presentación

1. Cuando yo era un niño, y de esto hace ya algún tiempo, y vivía, además, en una ciudad de provincias, una de mis actividades favoritas consistía en acompañar a mi madre a pasear por una de esas ferias ambulantes que, de pueblo en pueblo, iban vendiendo todo tipo de cacharros. En particular, me resultaban fascinantes aquellos personajes, llamados "charlatanes", graduados en marketing cum laude por la Universidad de la vida, que, debidamente pertrechados de un micrófono, o de cualquier otro aparato menos sofisticado de refuerzo auditivo (incluido el natural vozarrón norteño), promocionaban sus productos con argumentos, actuaciones y maniobras, de alcance cuasi-subliminal, basadas en las aparentes bondades y cualidades del objeto ofrecido al público. Era muy difícil sustraerse al encanto de aquellas peroratas envolventes y, de un modo u otro, el potencial cliente acababa convirtiéndose en un cliente real. Uno de aquellos "charlatanes", que repetía su actuación feria tras feria, era mi preferido, por su aplomo, su técnica y su seguridad. En una ocasión te vendía un pelador de limones de última generación. En otra, una cafetera ultra ligera para preparar el espresso italiano más genuino. O un ungüento para limpiar escopetas de caza. Se atrevía con todo lo que se le pusiese por medio. Para mí, lo de menos era que el producto resultase (o no) ser un bluff. Lo importante era el espectáculo. Y para él, lo importante, lo único importante, era vender.

2. Traigo a colación este recuerdo de mi infancia, porque me temo que vivimos ahora, muchos años más tarde, en un mundo de "charlatanes" de lo digital. De un tiempo acá han surgido, como champiñones tras la lluvia, infinidad de expertos en el mundo digital que pontifican, particularmente en esas nuevas ferias de la vanidad que son las redes sociales, acerca de la revolución digital, de cómo nos va a afectar, o nos está afectando, y, lo más importante, de cómo esos expertos nos van a ayudar (mediante una contraprestación razonable, por supuesto) a adaptarnos a ese nuevo y desconocido mundo. La mayoría son como mis admirados "charlatanes" de la vieja era. Ayer no sabían nada del mundo digital y hoy son los más avezados especialistas en la materia. Y mañana, por supuesto, cuando se les haya descubierto en su vacuidad, se pondrán a otra cosa. Busquen por las redes, contrasten currículos y experiencias, y comprueben cuántos charlatanes repiten constantemente el mismo mantra.

3. No pretendo desmerecer la relevancia de lo digital. Por el contrario, soy un firme convencido de que el mundo en el que estamos, y al que nos dirigimos, es, o será, un mundo dominado por lo digital. Tendremos que aceptar, de vez en cuando, timos de la estampita, como parece ser el metaverso, pero, de un modo u otro, siempre habrá quien se aproveche de las apariencias para hacer caja. Es la (parte negativa de la) naturaleza humana. Por eso es tan importante elegir bien las fuentes de información sobre la revolución digital y, como ahora nos ocupa, sobre su incidencia jurídica. Esta es la razón por la que recomiendo este Tratado de Derecho Digital, que analizaré a continuación. Conozco a quienes están detrás de la obra y puedo asegurar que, como indicaré más adelante, se trata de un trabajo realizado con realismo, honestidad,

conocimiento y una reflexión fundada en principios jurídicos y morales esenciales. Es una obra escrita por personas con autoridad y con capacidad de influenciar en este ámbito (no confundir con "influencers") y que del mismo modo que apuntan hacia los valores de lo digital, ponen el dedo en la llaga sobre sus limitaciones, oscurantismo y sus inevitables peligros.

4. A continuación, ofreceré una descripción de esta obra, que es algo extensa, porque la obra lo es, y lo hago con la mera finalidad de destacar sus virtualidades y, en su caso, contribuir a despertar un apetito por su lectura o su consulta, tanto en el ámbito privado como profesional. En cierto modo, al hacerlo, entiendo que alguno de ustedes pueda querer calificarme como un "charlatán" de esos de los que les hablaba antes. Tienen todo el derecho del mundo a hacerlo, pero, al final, lo importante es que el producto funcione. Y yo estoy convencido de que este producto funciona. No les puedo decir nada más. Como se indicaba en aquel anuncio de la era pre-digital, "busquen, comparen y se encuentran algo mejor, cómprenlo".

2. Planteamiento del *Tratado de Derecho Digital*

5. Los profesores Eduardo Valpuesta (Derecho mercantil) y Juan Carlos Hernández (Derecho administrativo) han coordinado esta obra que nos acerca al llamado «Derecho digital». El equipo de autores lo conforman fundamentalmente profesores (la mayoría de ellos de la Universidad de Navarra) de muy diversas disciplinas, no sólo jurídicas (hay también ingenieros, economistas, filósofos, arquitectos e incluso canonistas), y abogados especializados en estas materias. El libro abarca la regulación existente y la proyectada en esta materia que cada vez resulta más amplia, pues la mayoría de las relaciones sociales se realizan hoy en día transmitiendo datos digitales a través de medios digitales, y esto a menudo exige una norma especial diferente a las ya formuladas, que se basan en las relaciones presenciales.

6. Esta expresión de «Derecho digital» ya goza de cierta tradición en nuestro derecho, tanto entre la doctrina como entre las denominaciones de másteres específicos o de asignaturas optativas en planes de estudios universitarios, e incluso la reciente «Carta de Derechos Digitales» supone un cierto reconocimiento de su validez. Se sustituyen así otras denominaciones más antiguas que denominaban a este tipo de instituciones como «Derecho de las nuevas tecnologías» o «Derecho y TICs».

7. Pero si bien la denominación ya está asentada, lo que me parece más relevante de esta obra es que intenta justificar tal expresión con un punto de partida valorativo. Quizás pretender que exista una razón axiológica para aglutinar toda esta materia resulte un tanto pretencioso. Pero al menos el esfuerzo muestra un intento conceptualizador y justificativo que se agradece, sobre todo porque el punto de partida, los «datos digitales», me parece acertado y ciertamente muestra un elemento valorativo que puede fundamentar una cierta autonomía de este conjunto de materias.

8. Y es que, en efecto, en anteriores aproximaciones a estas instituciones se resaltaba el elemento técnico, como si las nuevas tecnologías fueran el objeto que exigía una cierta unidad de las materias y un nuevo punto de vista valorativo. Pero eso inevitablemente conducía a un batiburrillo de materias en cuya visión se exacerbaba el elemento tecnológico y disruptor como el que reclamaba una norma jurídica adecuada. Sin embargo, y como bien se resalta en la obra, las tecnologías son sólo un «medio», un objeto medial para todos los cambios y las nuevas realidades que requieren de nuevas normas. Lo relevante para aglutinar una nueva materia de derecho debe ser una institución puramente jurídica, y esa debe ser el «dato digital», que sí constituye un concepto jurídico que plantea nuevas exigencias de protección y, por lo tanto, nuevas normas específicas. Quizás más que en los «datos digitales» debería hacerse hincapié en el «tratamiento de los datos digitales», pero ciertamente la denominación apocopada resulta más gráfica y llamativa.

9. Para bien o para mal, en efecto, nuestra sociedad (la sociedad, la economía, y el derecho) se ha digitalizado. Ciertamente la sociedad no es sólo digital (aunque para algunos parece que se limita sólo a eso, a relaciones digitales), y sigue habiendo relaciones humanas interpersonales «presenciales» que son el objeto, en su vertiente jurídica, del derecho «clásico». Pero muchísimas relaciones con relevancia jurídica que antes se realizaban de forma presencial (o a distancia bajo formas de contacto

clásicas) ahora se han digitalizado: la identidad de los sujetos y la información se convierte en código binario y en aplicaciones informáticas, y todo se comunica y concierta «en la red». Así ocurre, por ejemplo, en muchos aspectos del comercio internacional, que ahora se celebra, se documenta y se monitoriza su ejecución por medios digitales.

10. Pero la digitalización no sólo supone traducir a código binario los datos y la información. Como se señala en esta obra, va mucho más allá, y crea un nuevo elemento con exigencias específicas de protección: el «dato digital». Cuando nació el «derecho digital» lo más relevante era el «comercio electrónico», y la «firma digital» constituía la forma de acreditar la identidad para realizar negocios jurídicos. Pero las técnicas digitales han ido mucho más allá, y lo relevante ahora no es negociar como se hacía antes (cambiando los medios tradicionales por medios digitales), sino tener cuantos más datos sea posible para diseñar aplicaciones informáticas y negocios que exploten las potencialidades de las nuevas relaciones sociales a través de internet. Al comerciante clásico internet le servía para establecer una página web desde la que vender sus productos y llegar a muchos más sitios; al comerciante actual, internet le sirve para recabar datos y diseñar los productos más adecuados a las necesidades de los clientes, y también para «bombardear» a éstos con publicidad sobre esos nuevos productos. Si antes los datos digitales constituían un medio para cumplir el negocio, ahora son más bien el «objeto» o «fin» para aplicarles técnicas de *big data* e inteligencia artificial, y con ellas «perfilar» a los clientes y crear los productos (bienes y servicios) adecuados. Y si para el comerciante clásico la firma digital constituía únicamente una forma de acreditar la identidad, en la economía actual ya no hay «firmas electrónicas» sino «identidades digitales» con muchas más connotaciones y posibilidades. Muchas cosas han cambiado desde la eclosión de la sociedad digital hasta nuestros días.

11. Toda la obra se estructura, por lo tanto, a partir de los datos digitales y de su tratamiento, y va combinando adecuadamente las explicaciones tecnológicas con las consecuencias jurídicas de la aplicación de las nuevas tecnologías a los datos. Y en relación con esto, querría resaltar la adecuada falta de triunfalismo en la valoración de lo que puede aportar la tecnología. En muchas ocasiones las nuevas tecnologías disruptivas se presentan como algo maravilloso y perfecto que va a solucionar muchos problemas de operativa material: la *blockchain*, el *big data* y la inteligencia artificial, los criptoactivos y la negociación operada por los *exchanges*, etc., sólo aportan ventajas y se supone que van a cambiar la forma de negociar y de operar en la sociedad digital. Pero la potencialidad real de todas estas tecnologías para operar un cambio relevante es muy relativa. En primer lugar, en su aplicación real padecen numerosos defectos de diseño, fallos operativos, y problemas de interoperabilidad, de forma que no son tan perfectas como se les presenta. En segundo lugar, a menudo lo que logran es facilitar ciertos aspectos materiales o procedimentales de la operativa clásica, pero dejan intactos los problemas jurídicos básicos. Y en tercer lugar, a veces crean muchos más problemas jurídicos que los materiales que solucionan. Pues bien, la obra que analizo ahora parte de eso y no resulta triunfalista o excesiva al presentar las novedades y facilidades que suponen las técnicas digitales. La parte más «anecdótica» y «sorprendente» de lo que permiten las nuevas tecnologías se presenta, sí, pero siempre para valorar seguidamente los problemas jurídicos que se plantean. En este sentido es verdaderamente un tratado de «derecho digital», no de «tecnología digital» ni de «sociedad digital». Se huye, también, de las palabrerías altisonantes y huecas, que resultan ilusionantes y compartidas por todos, pero sin contenido, a las que tan acostumbrados estamos en las propuestas de normas y en las exposiciones de motivos de algunas normas ya existentes: poco de lo que se dice en esta obra constituye un puro adorno, todo tiene un sentido.

12. La obra tiene cuatro partes: «Marco jurídico de la actividad digital», «Régimen jurídico de los datos digitales», «Digitalización de identidades, actividades y procesos» y «Competencia y propiedad intelectual en la sociedad digital». Aunque resulta manejable, tiene mucho contenido y sitúa todos los aspectos jurídicos que resultan afectados por la digitalización de la sociedad actual, y entre ellos muchos de los problemas que afectan actualmente al comercio internacional, que se realiza mayoritariamente a través de medios digitales. Se echa en falta algún desarrollo mayor de ciertos aspectos, pero ciertamente ello habría llevado a una obra mucho más voluminosa, y además podría haber asemejado al caos de materias que a veces

suponen otras obras que se refieren a esta temática. Más que un desarrollo exhaustivo de todos los temas (lo cual habría resultado casi imposible) se ha optado por establecer las líneas maestras de la regulación en cada materia, con esporádicas alusiones incluso a materias conexas. Hay que destacar el haber operado con la técnica de párrafos numerados, lo cual permite continuas remisiones entre partes de la obra, y además da lugar a un índice no sólo analítico, sino también de normas y de sentencias, que resulta sumamente útil. Este índice muestra, además, la buena coordinación de los contenidos, lo cual es de agradecer en una obra en la que, necesariamente, intervienen tantos autores diversos.

3. Marco jurídico de la actividad digital.

13. La primera parte de la obra trata aspectos generales del derecho digital. Se divide en cuatro Capítulos. El primero de ellos lleva como título «Concepto y normativa sobre derecho digital», y comienza con una breve «aproximación» al concepto y características del derecho digital y su normativa, redactada por Eduardo Valpuesta. Sirve para centrar los conceptos básicos: el objeto del derecho digital lo constituyen los «datos digitales»; los sujetos, los operadores de la sociedad digital; los medios de transmisión, los diversos medios digitales; y los resultados, la digitalización de procesos (que se mantienen básicamente iguales, pero ejecutables telemáticamente) y la aparición de nuevas actividades (como las diversas aplicaciones tecnológicas en materia de financiación o de operativa comercial). Un énfasis especial debe realizarse en el tratamiento que se efectúa de los llamados «puertos seguros» en la actuación de los intermediarios de servicios de la sociedad de la información: tanto la normativa comunitaria como la española exoneran a tales intermediarios de responsabilidad por los posibles contenidos ilícitos que alojen o transmitan, siempre que se cumplan una serie de requisitos (desconocimiento y cesación en el alojamiento o transmisión cuando sean advertidos).

14. A continuación se tratan diversos aspectos específicos en materia de derecho internacional privado y derecho fiscal. La parte de derecho internacional privado corresponde a Alberto Muñoz Fernández, y resulta de vital importancia porque buena parte de la actividad digital es transfronteriza, y por eso resultan relevantes los criterios de conexión para determinar las reglas sobre derecho aplicable y tribunales competentes. No se repiten las reglas generales, sino que el autor realiza referencias específicas a las especialidades que plantea la actuación y contratación por internet. En este sentido, se dedica una especial atención en cuanto a los tribunales competentes cuando se ha producido un daño extracontractual a través de la red, algo que plantea numerosos problemas por la diversidad de posibles criterios de conexión que surgen. En cuanto a la parte de fiscalidad digital corre a cargo de Antonio Vázquez del Rey Villanueva, que trata específicamente de la tributación por IVA en el mercado de bienes y servicios digitales, y en la tributación internacional de los beneficios empresariales. Este segundo aspecto es uno de los que más ha llamado la atención en los últimos años, con la polémica acerca de cómo los grandes operadores de la economía digital aprovechan las estrategias de tributación y cómo los diversos Estados intentan gravar las operaciones realizadas materialmente en cada territorio. Se referencian los trabajos que se están llevando a cabo en la OCDE, la UE y la ONU, y se detalla la solución actual seguida en España con el Impuesto sobre determinados servicios digitales.

15. Este primer Capítulo termina con un apartado dedicado a la desinformación y las noticias falsas (*fake news*), de autoría de Andrea Cocchini. Al principio llama la atención la ubicación sistemática de esta parte, pero ciertamente se trata de una materia que podría tratarse en otros muchos lugares sin encontrar acomodo natural en ninguno de ellos (o, al menos, un acomodo menos sorprendente como el que ahora tiene). Y es que las *fake news* no son algo puramente jurídico, pero sí caracterizan la operativa real de internet, y despliegan efectos en aspectos jurídicos muy diversos (ciberseguridad, ciberterrorismo, influencia en la opinión pública, etc.). La cuestión conecta con el derecho internacional público, y por eso se hace la oportuna referencia al Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas (2017) o al Plan de Acción contra la Desinformación aprobado en la Unión Europea (2018), e incluso a los esfuerzos desplegados igualmente por la Unión Europea para combatir la desinformación sobre las vacunas contra la COVID-19.

16. El segundo de los Capítulos se refiere a Internet y a otras tecnologías disruptivas, porque

justamente es preciso conocer cómo operan las tecnologías que se utilizan en la sociedad digital, para luego poder comprender los problemas que se generan. La parte relativa a Internet se desarrolla por Joslay Polanco Medina, que expone cómo fue el nacimiento y el desarrollo de Internet, desde el Arpanet ideado con fines militares a la actual web 2.0. La autora se centra igualmente en los retos actuales en la «gobernanza» de internet, con las dos posturas básicas de «ciberpaternalismo» y «ciberlibertarismo»; se trata de una discusión inacabable que sigue sin tener una respuesta clara, y hace que toda la normativa proyectada se debata en cuánto y hasta dónde regular para introducir una mínima seguridad jurídica en las relaciones a través de medios digitales. En la segunda parte de este capítulo, Eduardo Valpuesta realiza una pedagógica exposición acerca de tres tecnologías disruptivas que permiten todo el desarrollo de aplicaciones y relaciones negociales que conocemos hoy en día: el *internet of things*, la técnica de la cadena de bloques (*blockchain*), y el *cloud computing*. Obviamente todo esto iría ligado a las técnicas de *big data* y de inteligencia artificial, que por su importancia se tratan en un capítulo aparte. Los dispositivos de *internet of things* permiten obtener y alojar millones de datos de muy diverso tipo (meteorológicos, urbanos, domésticos, personales de salud, etc.), que permiten luego la operativa de *big data* y el desarrollo de muchísimas aplicaciones informáticas. La *blockchain*, tan de moda actualmente por -entre otras razones- el uso de los criptoactivos, se centra adecuadamente como una técnica de alojamiento de datos que sirve para muchos fines, y se explican las técnicas de minado y los actuales desarrollos de la *blockchain*, con la proliferación de «cadenas de bloques» privadas y permisionadas que pueden cumplir mejor la normativa aplicable. Por último, el *cloud computing* es una técnica que permite alojar millones de datos en servidores ajenos a los propios del usuario, lo cual proporciona gran capacidad de computación y además el acceso a los datos desde cualquier lugar. Se trata de técnicas todas ellas necesarias para el actual desarrollo de las aplicaciones informáticas.

17. El tercer Capítulo trata de los «operadores» y de los «modelos de negocio» en internet, y ha sido elaborado por Pablo González Espejo, Núria Porxas Roig y Nerea Sanjuán Rodríguez (excepto en la parte relativa a los delitos de odio). La primera parte se refiere al régimen de los operadores tanto de comunicaciones electrónicas, regidos por la Ley General de Telecomunicaciones (actualmente en trance de reforma), como de comunicaciones audiovisuales, sometidos a la Ley General de la Comunicación Audiovisual, y también a los «prestadores de servicios de la sociedad de la información», regidos por la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico. La referencia a estas regulaciones, a los requisitos de autorización y de operativa en cada uno de estos ámbitos, es sumamente necesaria porque a veces se obvia este marco normativo que justifica otros aspectos del régimen jurídico del derecho digital. La segunda parte de este Capítulo trata de los «modelos de negocio» tanto en el ámbito de las telecomunicaciones como en el sector audiovisual o de las comunicaciones electrónicas. Aquí se desarrolla la evolución desde las páginas web hasta las modernas plataformas que articulan formas de negocio muy diversas (*market-places*, intermediación, alojamiento, economía colaborativa, etc.), con el surgimiento además de las «redes sociales» como una nueva forma de relación social, y la aparición de otros actores sectoriales como los *influencers*.

18. Termina este tercer Capítulo con una breve referencia a los delitos de discurso de odio en las redes sociales, como una forma de escenificar uno de los ejemplos concretos de actos con relevancia jurídica que se desarrollan a través de estos medios digitales de comunicación. El enfoque de este apartado, a cargo de Ana Azurmendi, no es el propio del derecho penal (el «derecho penal digital» se desarrolla en otra parte de la obra), sino más bien el comunicacional, mostrando cómo internet facilita la difusión de estas ideas, y lo difícil que resulta realizar un control y una protección eficaz frente a estas conductas.

19. El cuarto Capítulo de esta primera parte recoge una serie de colaboraciones que se relacionan con la fundamentación antropológica del derecho, y con aspectos generales de cómo afecta este nuevo mundo digital a los derechos de la personalidad. De nuevo se pone la prioridad sobre la persona y no sobre la tecnología, y se tratan esos múltiples puntos en que hay que someter la potencialidad de la tecnología a las exigencias de la libertad y dignidad del ser humano. Una primera parte se refiere a la llamada «Ética digital», y cómo los desarrollos de inteligencia artificial se

pueden alinear con la ética de la virtud. Redactada por Alejo Sison y Dulce Redín, concluye que las virtudes intelectuales y morales deben ayudar a garantizar que la relación entre el ser humano y la inteligencia artificial no sólo sea eficiente, sino que también perfeccione al ser humano y se ordene adecuadamente para contribuir a la buena vida.

20. La obra no trata todas las posibles afectaciones de la sociedad digital a cada uno de los derechos de la personalidad, posiblemente porque ello supondría una extensión muy superior a la posible en una obra general. La materia que se elige para ejemplificar esta afectación es la videovigilancia digital, y cómo la misma puede tener incidencia en derechos como la intimidad, pero también la dignidad y la libertad humana. Ha sido elaborada por Asunción de la Iglesia, que hace hincapié en la normativa que regula la videovigilancia, tanto la general contenida en la Ley Orgánica de Protección de Datos, como la sectorial en cuanto a la videovigilancia en las relaciones laborales o para la seguridad privada. La autora pone de manifiesto no sólo la posible afectación a facetas como la intimidad, el honor o la propia imagen, con la jurisprudencia recaída en estas materias, sino también otros aspectos menos evidentes pero igualmente relevantes, como el llamado «*chilling effect*» o efecto inhibitorio: la monitorización constante de nuestras vidas por la videovigilancia (y, añadimos nosotros, por los instrumentos de *internet of things*, las redes sociales, nuestro tráfico en la red, etc.) limita nuestra libertad porque somos conscientes de que estamos controlados. Y todos los datos que cabe obtener sobre nosotros, utilizados por las personas o con fines adecuados, pueden suponer un efecto devastador.

21. Finaliza esta cuarto Capítulo con otros ejemplos de afectación de derechos de la personalidad, tan relevantes como frecuentemente olvidados, «Menores y redes sociales» y el «Rastro digital». Las redes sociales, en efecto, son utilizadas a menudo por menores de edad, con o sin consentimiento de sus cuidadores, y de hecho está demostrado cómo afectan a sus conductas y crean nuevos problemas de relaciones sociales. La redacción de esta parte corre a cargo de Carmen Pérez Dios, que pone de manifiesto que no se trata sólo del uso directo de las redes, sino incluso de la dudosa legitimidad del uso de sus imágenes por sus progenitores o por terceros. La autora expone la normativa aplicable, tanto la Ley de Protección Jurídica del Menor como la Ley Orgánica de Protección de Datos. Un segundo aspecto que se trata es el llamado «rastro digital» y «patrimonio digital»: resulta un tanto macabro, pero la potencialidad que tiene internet hace que deba regularse incluso el uso de los datos digitales cuando fallece el sujeto al que se refieren. La autora de este apartado, Verónica San Julián, expone la problemática general y desarrolla la normativa aplicable, que por ahora sigue siendo la general de la Ley Orgánica de Protección de Datos. Se hace referencia a la primera regulación española de esta materia en el ámbito autonómico, que es la Ley catalana de Voluntades Digitales.

4. Régimen jurídico de los datos digitales

22. La segunda parte de la obra es la dedicada al régimen jurídico de los datos digitales. Se divide en cuatro Capítulos, dos de ellos con contenidos plenamente jurídicos, y los dos últimos con contenidos fundamentalmente técnicos (o «tecnológicos»): qué son los «datos digitales» y cuál es su régimen jurídico general; la normativa de protección de los datos personales; el tratamiento de datos mediante técnicas de *big data* y el desarrollo de aplicaciones de inteligencia artificial; y la ciberseguridad de los datos digitales. Como en la primera parte, muchos de los conceptos que aquí se desarrollan se tratan de forma general, y es en las dos partes siguientes de la obra donde se exponen aplicaciones concretas y «casos de uso» de cada una de estas problemáticas.

23. El primer Capítulo de esta parte trata los «Fundamentos del régimen jurídico de los datos digitales», y ha sido redactado por Leticia López-Lapuente. El «dato digital» será cualquier representación simbólica de un atributo o variable cuantitativa o cualitativa que se contiene y representa utilizando el sistema binario de unos (1) y ceros (0), y la autora expone las distinciones básicas entre datos personales *vs.* no personales, datos personales anonimizados *vs.* seudonimizados, y datos *vs.* metadatos. A continuación se hace referencia a la Estrategia europea de datos y a las normas ya existentes, como el Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la UE, y la Directiva 2019/1024, relativa a los datos abiertos y la reutilización de la

información del sector público (Directiva de *open data*), que promueven la circulación y utilización de datos no personales (lo cual incluye los «personales anonimizados»). El Capítulo finaliza con el reflejo de las líneas fundamentales de la propuesta de noviembre de 2020 de gobernanza del dato, que busca establecer mecanismos para ampliar la reutilización de datos del sector público, adoptar medidas para generar confianza en los intermediarios de datos y para facilitar la cesión de datos con fines altruistas, y crear un mecanismo europeo para coordinar y dirigir los aspectos horizontales de la gobernanza.

24. El Capítulo segundo de esta parte, redactado fundamentalmente por Juan Carlos Hernández, expone con cierto detalle el régimen jurídico de la protección de datos personales, contenido ahora en el Reglamento General de Protección de Datos y en la Ley Orgánica de Protección de Datos Personales. Es una de esas materias muy relevantes en la sociedad actual que, sin embargo, no suele ser objeto de explicación en nuestras Facultades de Derecho. Esta normativa entronca con buena parte de los derechos fundamentales de las personas (dignidad, libertad, privacidad, propia imagen, etc.), y se encuentra ante la paradoja de la necesidad de protección de unos activos cuyo uso es, sin embargo, de vital importancia para el desarrollo comercial de muchas empresas. Nos hallamos, así, ante la «lucha» de grandes empresas por obtener datos personales de sus clientes y poder usarlos, todo ello de forma legítima. Obtención y uso que tiene como finalidad la de diseñar los productos y servicios adecuados, y luego ofrecerlos a todos los sujetos, pero también con especial énfasis a ese mismo cliente que cedió esos datos. Las formas realmente «abusivas», en muchos casos, en que se obtiene la cesión de datos personales han exigido esta regulación, que dentro del ámbito europeo ha cristalizado en el Reglamento General de Protección de Datos, que ha sido tomado universalmente como uno de los paradigmas de regulación en este ámbito más acertados y equilibrados. Este Capítulo va reflejando con detalle el objeto de la protección y su ámbito de aplicación; los principios generales del tratamiento de datos; las bases jurídicas de dicho tratamiento (fundamentalmente, el consentimiento del interesado); los derechos de los interesados (con especial referencia al derecho al olvido, o al derecho a la portabilidad de datos); la distinción entre el «responsable» del tratamiento y el «encargado» del tratamiento; las obligaciones, medidas e instrumentos materiales de protección; y las autoridades de supervisión y control. No falta la exposición del régimen de transferencia internacional de datos, con la referencia a la necesidad de comprobar el nivel de protección adecuado y similar al Reglamento para transferir datos a otros países, y la actual situación del «escudo de privacidad» con Estados Unidos de América.

25. El Capítulo termina con uno de esos *excursus* que van trufando esta obra y la dotan de originalidad y riqueza, el tratamiento de la protección de datos personales en la Iglesia, realizado por Jorge Otaduy. Y es que la protección de datos personales abarca a todos los ámbitos, incluidos el religioso, y además en el ámbito canónico la privacidad de las personas también es entendida como un bien jurídico. Se expone la doctrina de la STS 22 febrero 2021, que consideró proporcionado que una entidad religiosa conservara el nombre y apellidos, y la fecha de incorporación y salida, de uno de sus desasociados; y no proporcionado, en cambio, el conservar igualmente la congregación local a la que había pertenecido, la fecha de nacimiento o el sexo.

26. Como queda expuesto, la normativa de protección de datos personales es objeto de frecuentes alusiones en otras partes de la obra, pues constituye uno de los puntos centrales del derecho digital con diversas manifestaciones: protección de datos personales en el almacenamiento en la nube, en la transmisión de datos realizada por medio de instrumentos de IoT, en mecanismos de videovigilancia, en el uso de redes sociales, en las comunicaciones comerciales, etc. Posiblemente la sensación generalizada que hoy tenemos es la de que toda la protección formal que nos brindan las normas existentes no impide que nuestra privacidad está seriamente amenazada, en parte por las exigencias y limitaciones de la tecnología, en parte por las necesidades especiales que imponen excepciones en materia de seguridad u orden público, y en parte también por el propio uso que las personas realizamos de nuestros datos. Y, por supuesto, nos queda también el miedo de que una empresa que infrinja la normativa existente pueda causar un daño irremediable, por mucho que incluso sea apreciada la ilicitud de su conducta y sancionada. ¿Cuántos casos de obtención y uso ilícito de datos como el de *Cambridge Analytica* no habrán sucedido sin que seamos conscientes de ello?

27. El Capítulo VII, tercero de esta segunda parte, trata del *big data* y de la inteligencia artificial. Se divide en dos grandes apartados, uno más referido a aspectos tecnológicos, y otro más jurídico. El primero de ellos ha sido redactado por miembros del Instituto de Ciencia de los Datos e Inteligencia Artificial de la Universidad de Navarra (Jesús López-Fidalgo, Iván Cordón Medrano, Leire Alegria, Álvaro Cía, Stella Maris Salvatierra, Pablo Urruchi y Edgar Benítez), y parte claramente de que hoy por hoy la inteligencia artificial se halla en un estadio embrionario, y consiste más en programación para alcanzar resultados determinados que verdadera «creación» por las máquinas de resultados basados en un razonamiento propio (de la máquina). Y es bueno que sea así, a mi juicio, porque el día en que los ordenadores puedan tomar decisiones propias perderemos en absoluto el control de sus actos, y la garantía del sometimiento de éstos a reglas jurídicas y morales. Se realiza referencia, en primer lugar, a aspectos generales de cómo operan el *big data* y la inteligencia artificial, mediante técnicas de programación más bien sencillas, hasta las más complejas (y, por ahora, poco avanzadas) de *machine learning* y *deep learning*. Se pone correctamente el énfasis en los problemas de posibles «sesgos» al usar los datos o al «entrenar» a las máquinas, algo cuya evitación resulta muy difícil de llevar a la práctica con éxito, y de la posible «falta de transparencia» de los procesos o de los algoritmos utilizados para alcanzar un resultado. El Capítulo continúa con una exposición básica de aspectos de estadística, necesarios para entender cómo opera el *big data* y qué razonamientos lógicos se tienen en cuenta para la toma de decisiones. Una tercera parte se refiere a los «modelos», y realiza una exposición básica tanto de los «modelos estadísticos» (representaciones matemáticas de los datos observados) como de los modelos utilizados en el *machine learning* (regresión lineal múltiple, árboles de decisión, regresiones logísticas, algoritmos, o validaciones cruzadas). Se finaliza con unas reflexiones generales relativas al *big data* en los ámbitos jurídico y de las ciencias sociales. En ella se pone de manifiesto cómo el *big data* puede revelar sesgos cognitivos en el tribunal, o determinar la identidad de una persona por medio de su «huella digital», de los distintos elementos de su personalidad que va poniendo de manifiesto en sus interacciones digitales.

28. Un segundo apartado de este Capítulo se refiere a aspectos jurídicos de la inteligencia artificial. Lógicamente la primera colaboración expone la propuesta de regulación de inteligencia artificial presentada por la Comisión Europea en abril de 2021, y se realiza por María Teresa Gil Bazo. Se parte de la definición de inteligencia artificial como «el *software* que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa». La autora destaca los cuatro niveles de evaluación del riesgo: inaceptable; alto; limitado; y mínimo. Entre otros supuestos es inaceptable, y está por lo tanto prohibida, la inteligencia artificial que utiliza de forma indiscriminada la identificación biométrica de sujetos en áreas públicas. Las técnicas que suponen un riesgo alto están reguladas, sólo pueden ser realizadas por entidades autorizadas para ello y con los sistemas que se autoricen; las que supongan riesgo limitado pueden realizarse siempre que se informe adecuadamente; y las que supongan riesgo mínimo está autorizadas sin restricciones. La segunda aproximación se realiza por María Cruz Díaz de Terán Velasco, y versa sobre los códigos de conducta responsable en productos de inteligencia artificial. A falta de regulación, en la actualidad existen una serie de recomendaciones de buenas prácticas, como las *Ethics Guidelines for Trustworthy Artificial Intelligence*, la *AI HLEG*, o las *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del RGPD*, que muchas empresas que desarrollan productos de inteligencia artificial cumplen para asegurar una actuación ética y jurídicamente adecuada. La autora expone un ejemplo concreto de una empresa que ha diseñado un producto que realiza análisis de personalidad, preferencias, valores y competencias a partir de textos en el lenguaje natural de las personas, y transcribe los «Principios de comportamiento responsable» de ese producto. La tercera colaboración en esta parte corresponde a Pablo Gómez Blanes, que trata el tema de los robots. Entiende por «robot» al «"intelecto sintético", autónomo de su programador y de su titular o usuario, que, analizando los datos percibidos por sensores, interactúa en el entorno sin necesidad de guía ni de control alguno». La cuestión fundamental que surge en esta materia es la responsabilidad por los posibles daños causados por el robot. Como señala el autor, la postura que apareja

una «personalidad jurídica» al robot resulta minoritaria, y la más generalizada es la que defiende la responsabilidad solidaria de los distintos operadores jurídicos (fabricante, programador, proveedor, titular, usuario), sin perjuicio de una posterior depuración por vía de regreso si cabe determinar cuál de todos ellos es el sujeto causante del fallo o error. Posiblemente se generalizará la exigencia de contratación de un seguro de responsabilidad civil (tanto más «obligatorio» y «cuantioso» en función del potencial daño que pueda causar el robot), que asegure una indemnidad al perjudicado. El apartado finaliza con una referencia a las *Smart cities*, elaborada por Elena Lacilla Larrodé y César Martín Gómez. La «ciudad inteligente» es la que aplica las Tecnologías de la Información y la Comunicación para la mejora de la calidad de vida y la accesibilidad de sus habitantes, y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente. Los autores van exponiendo diversas aplicaciones de inteligencia artificial que logran este propósito en varios ámbitos: seguridad (videovigilancia, ciberseguridad de dispositivos IoT, regulación de intensidad de luz, etc.); gestión de recursos (agua, residuos y aire); energía (redes inteligentes de energía, edificios consumo cero, etc.); y transportes y movilidad (vehículos conectados, uso de drones, uso de geolocalización para estudiar la movilidad de los ciudadanos, etc.). También exponen la necesidad de contar con centros de gestión de datos adecuados, la normativa aplicable y los organismos que implantan y supervisan estos sistemas.

29. El último Capítulo de esta parte se refiere a la ciberseguridad, y engloba igualmente aspectos tecnológicos y jurídicos. La enorme cantidad de aparatos conectados a Internet hace necesario que todos ellos cuenten con las medidas de seguridad adecuadas para evitar ataques informáticos que bien roben o manipulen datos, bien bloqueen o accedan al aparato o algunas de las aplicaciones con fines delictivos. Esto implica, además, toda una obligada política de *compliance* de ciberseguridad, de modo que todas las empresas deben contar con los sistemas de seguridad adecuados para evitar razonablemente los ataques informáticos; sistemas que deberán ser tanto más sofisticados cuanto más y más complejos o sensibles sean los datos personales que se manejen. Las técnicas digitales facilitan muchos procesos, pero también llevan aparejados numerosos nuevos peligros.

El primer apartado de este Capítulo se refiere a los aspectos técnicos de la ciberseguridad, y ha sido redactado por Diego Urruchi Mohíno. Se parte de que no existe ningún sistema informático absolutamente seguro, y que los sistemas serán seguros si garantizan la integridad, la confidencialidad y la accesibilidad de los datos. A continuación, se exponen los diversos tipos de amenazas o ataques que pueden producirse: de *hardware*, de observación, de penetración, de *software* dirigidos a *hardware*, de red, contra el sistema de nombres de dominio, contra el enrutamiento entre dominios del *Border Gateway Protocol*; y de *software*. También se exponen unos fundamentos de criptografía, de técnicas y herramientas para cifrar los mensajes y garantizar así su confidencialidad. Y por último se tratan los diversos tipos de *malware* o programas maliciosos, que incluyen también los «programas potencialmente no deseados», fragmentos de código que forman parte de un código útil descargado por el usuario, y que se instalan en el ordenador a menudo sin el conocimiento o consentimiento expreso del usuario.

El segundo apartado del Capítulo, a cargo de Eugenia López Jacoiste, explora los aspectos jurídicos de la ciberseguridad desde la óptica del Derecho internacional. Si bien a menudo enfocamos la ciberseguridad como un problema de usuarios (bien particulares, bien empresas), constituye también un problema de primer grado en el ámbito del Derecho internacional, pues Internet se ha usado a menudo como forma de atentar contra la paz y la seguridad internacionales. Por eso todos los Estados y organizaciones supraestatales establecen e implantan sistemas de ciberdefensa tanto pasiva (para detectar las causas de la amenaza y combatir el mal funcionamiento del sistema) como activa (perseguir a los atacantes en sus propias redes). El trabajo hace referencia a las principales características de los planes de ciberseguridad de Reino Unido, Estados Unidos de América, España y, con especial detalle, la Unión Europea. Además, se exponen las diversas reglas existentes en el Derecho internacional para evitar los ciberataques y determinar la responsabilidad en el caso de que se produzca alguno de ellos, como las recogidas en el Manual de Tallin 2.0 sobre Derecho internacional aplicable a las operaciones cibernéticas, o las aplicadas por la Comisión de Derecho Internacional. Por último se tratan las defensas que cabe adoptar frente a los ciberataques (tanto provengan de un Estado como de una entidad no estatal), que básí-

camente consistirán en contramedidas (medidas de autotutela que no suponen uso de la fuerza, como sanciones y embargos), pero también pueden suponer el uso de la fuerza si el ataque cibernético puede ser considerado un «ataque armado» de gravedad, y se cumplen los requisitos de la legítima defensa.

5. Digitalización de identidades, actividades y procesos

30. Una vez expuestos los aspectos generales del Derecho digital, y el concepto y régimen de los datos digitales y de su tratamiento, la Parte Tercera de este *Tratado* estudia cómo se han digitalizado las identidades, los procesos y las actividades. La mayoría de las relaciones interpersonales se llevan a cabo ahora por medios digitales, de forma que buena parte de lo que antes se hacía presencialmente y con documentación y bienes físicos hoy se realiza a distancia y con documentos y medios electrónicos. Y, como se señalaba en las primeras páginas de esta obra, en algunos casos esta digitalización mantiene la esencia de lo que antes se hacía (por ejemplo, un proceso judicial gestionado por medios digitales sigue los mismos trámites y documentación, aunque se incorpore a mecanismos digitales), pero otras cambia por completo la forma de actuar, o crea nuevas posibilidades que antes ni siquiera se podían imaginar. Esta parte es la más extensa de la obra, porque supone el estudio de muchos aspectos concretos del Derecho que se han digitalizado, y comprende cuatro grandes Capítulos que estudian la digitalización de identidades, de procesos y de actividades y contratos, así como la cibercriminalidad.

31. El primer Capítulo de esta parte trata la identidad digital, la firma electrónica y la reputación *online*. Un primer apartado, a cargo de Leticia López-Lapuente, trata los aspectos de identidad digital y firma electrónica. La «identidad digital» constituye un nuevo concepto, e incluso una nueva categoría jurídica, pues no se corresponde exactamente con la identidad física ni la personalidad jurídica. Opera, desde luego, efectos de «identificación», pero también de asignación de atributos por parte del titular, además en muchos casos sin una comprobación «oficial» de la veracidad de la identidad ni de las características asociadas. Especial interés tiene la propuesta de establecimiento de un marco para la Identidad Digital Europea, presentada en junio de 2021, porque ésta sí permitirá gestionar de forma segura y «soberana», a voluntad del titular, los atributos de identidad que él desee por medios digitales. El problema de todos estos mecanismos es que todavía la tecnología no está tan avanzada y segura como se quiere hacer parecer, y sobre todo que debe crearse un sistema interoperable con todas las aplicaciones y medios de transmisión, lo cual complica mucho el diseño y operatividad. Se expone, igualmente, el sistema actual de firma electrónica por medio de los actualmente llamados «servicios de confianza», regulados en el Reglamento EiDAS y en la Ley española 6/2020, y el valor probatorio en juicio de los documentos electrónicos.

32. Una segunda parte de este Capítulo, redactada por Borja Sainz de Aja, trata sobre la reputación *online*, que es la consideración que la comunidad de internautas tiene de una persona física o jurídica. Al igual que Internet permite crear una o varias (incluso muchísimas) identidades específicas, también dota de especiales características a cada identidad, basadas además no siempre en la propia voluntad del «identificado». Nuestra huella digital, los datos de navegación, y lo que los demás hacen constar en Internet sobre nosotros, conforman una identidad digital y una reputación *online* con vida propia, no siempre controlable por el titular. En esta colaboración se parte de la posible interferencia entre la libertad de información y de expresión, por un lado, y el derecho al honor y a la propia imagen, por otro. A partir de ahí se van tratando los diversos «grupos de casos digitales» de reputación *online*: comentarios de usuarios sobre las prestaciones ajenas, vindicación *ad personam* (comentarios negativos frecuentes que exceden de lo razonable en una práctica informativa), utilización inconsentida de la imagen, uso de caricaturas, o manifiestos en la red atribuidos sin control a multitud de sujetos. Las normas generales de derecho privado, o específicas de competencia desleal u otros ámbitos, sirven para reprimir los ilícitos que se producen en este campo, tratándose igualmente la posible responsabilidad de los intermediarios de los servicios de la sociedad de la información.

33. Los dos siguientes Capítulos de esta parte del *Tratado* se refieren a la digitalización de procesos y de actividades y contratos, son de los más largos de la obra y tratan muy diversos aspectos

en que la digitalización se ha aplicado a procedimientos y/o actividades y contratos. En buena medida ambos Capítulos suponen aplicaciones de todo lo anterior (características de los datos digitales, formas de digitalización, actuación de distintos operadores digitales, operativa de tecnologías disruptivas, etc.) en los más variados campos de lo jurídico: administrativo, procesal, contratación privada y financiación, laboral, financiero, etc. La sistematización en dos capítulos es puramente convencional, una simple forma de agrupar todos estos aspectos con un cierto orden expositivo. El Capítulo sobre digitalización de procesos se refiere básicamente a la operativa digital sobre procesos jurídicos, y el Capítulo sobre digitalización de actividades y contratos a la transformación digital en la actividad contractual.

34. El Capítulo relativo a los procesos se divide en nueve apartados. El primero de ellos trata algunas cuestiones de derecho digital en materia de Administraciones Públicas, y se elabora por Juan Carlos Hernández. El autor estudia el principio de «datos abiertos» y la política de reutilización de la información pública, que busca elaborar y garantizar el acceso a bases de datos públicos que resulten comparables; la gobernanza de la interoperabilidad y el esquema nacional de interoperabilidad (la disponibilidad y el uso de información sólo son posibles si técnicamente se garantiza el intercambio electrónico de datos); y el Esquema Nacional de Seguridad aplicado para la ciberseguridad de las Administraciones Públicas. Un segundo apartado, a cargo de Eduardo Valpuesta, realiza una breve referencia a los llamados procesos de *RegTech* y *SupTech*, la implementación de tecnologías digitales en la labor que realizan las empresas de monitorización del cumplimiento de la normativa aplicable, y a la que realizan las Administraciones Públicas para comprobar que las entidades reguladas y supervisadas cumplen la citada regulación.

El apartado tercero se refiere a la digitalización en los procesos de administración de justicia. Faustino Cordón se encarga de exponer tres aspectos concretos de la digitalización en el proceso civil: la prueba por medios digitales, que incluye el valor probatorio de los documentos electrónicos; el expediente judicial electrónico; y la subasta electrónica. Julio Muerza redacta la parte relativa a la digitalización en la administración de justicia penal, en la que estudia las diversas medidas de investigación tecnológicas incorporadas a la Ley procesal penal mediante la Ley Orgánica 13/2015: la interceptación de comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicas de captación de la imagen, de seguimiento y de localización; el registro de dispositivos de almacenamiento masivo de información; el registro remoto sobre equipos informáticos; y las medidas de aseguramiento. Por último, Mª. Victoria Sánchez Pos desarrolla el uso de medios digitales para la operativa de los medios alternativos de solución de controversias, algo que ya lleva muchos años aplicándose, incluso con iniciativas pioneras en distintos ámbitos, como el sistema europeo *online* de solución de conflictos en materia de consumo. En cierta relación con estos ámbitos de administración de justicia, un cuarto apartado del Capítulo trata el llamado *LegalTech*, la aplicación de tecnologías digitales en el ámbito del ejercicio de la abogacía. Redactado por Eduardo Valpuesta, huye adecuadamente de algunos de los triunfalismos que se han manifestado en esta materia para exponer cómo se trata de aplicaciones de inteligencia artificial débil para la gestión de documentación y de servicios jurídicos; sistemas que sirven para agilizar aspectos más mecánicos, pero que nunca suplen la labor ordenadora y creativa que luego debe aplicar todo jurista.

35. Los dos siguientes apartados de este Capítulo se refieren a la aplicación de tecnologías digitales en los ámbitos registral y de la fe pública. Se han redactado por Luis Javier Arrieta Sevilla. Es evidente que la digitalización de los datos y la posibilidad de transmisión electrónica de millones de datos documentos facilita muchos aspectos de gestión documental en estas materias. En cuanto a los registros públicos, se estudia la presentación remota de documentación por medios telemáticos, la interoperabilidad entre la información territorial y la que consta en el Registro de la Propiedad, la digitalización del contenido del registro, y los mecanismos de publicidad formal por medios digitales. También se realiza una referencia al posible uso de técnicas de *blockchain* para la llevanza de los registros públicos, algo sobre lo que el autor manifiesta sus razonables dudas, porque en ellas difícilmente pueden implementarse toda una serie de garantías jurídicas que se exponen. En el ámbito de la fe pública se estudia la firma electrónica de los notarios, el documento notarial electrónico,

los deberes de colaboración con la administración electrónica, o la legitimación notarial de firmas electrónicas. En los inicios del derecho digital se propuso por algunos que las nuevas tecnologías harían desaparecer el papel de los notarios; sin embargo, está claro que la tecnología podrá facilitar muchas cosas, pero no garantiza ciertos aspectos (la capacidad de las partes, o la legalidad de las declaraciones de voluntad emitidas) cuya encomienda a los notarios sigue siendo útil y adecuada.

La siguiente parte en este Capítulo trata la digitalización de procesos en sociedades mercantiles. Patrick O'Malley expone cómo puede operar la digitalización en la constitución y en la publicidad registral de sociedades mercantiles, así como en la llevanza de registros de socios. En este ámbito la Directiva 2019/1151, aún pendiente de trasponer en España, exige establecer un procedimiento que permita digitalizar la constitución de sociedades, la creación de sucursales y la consulta al registro mercantil, si bien sin imponer esta vía telemática como modo único de operación. Jorge Noval se encarga de desarrollar cómo opera la digitalización en las comunicaciones sociedad – socio (incluyendo la regulación de la web corporativa), y en la operativa de los órganos sociales (convocatoria y celebración de la junta general y de los órganos de administración). La situación creada inicialmente por la pandemia supuso un incentivo importante para acelerar la implantación de este tipo de soluciones tecnológicas, pero siguen abiertas muchas cuestiones acerca de cómo compaginar estos medios con las necesarias garantías jurídicas, de las que se ocupa cumplidamente el autor.

36. Termina este Capítulo con dos colaboraciones sobre juego *online* y sobre aplicaciones de inteligencia artificial en materia de salud. El primero de estos apartados, desarrollado por Inmaculada Baviera, expone los problemas jurídicos que plantea tanto el juego *online* (apuestas deportivas, o práctica *online* de juegos como el bingo, el casino o el póquer) cuanto los llamados *eSports* (competiciones de videojuegos, que incluso están organizadas actualmente en distintas Ligas y torneos). Las aplicaciones de inteligencia artificial en materia de salud han creado el llamado *eHealth* y *mHealth* (*electronic Health* y *mobile Health*, entendida esta última como el uso de aparatos móviles para monitorizar o asesorar en materia de salud). Eduardo Valpuesta se encarga de la elaboración de esta parte, y pone de relieve los problemas de falta de interoperabilidad entre los distintos aparatos y sistemas de almacenamiento de datos, y sobre todo los de tratamiento de estos datos de salud, que mayoritariamente resultan «categorías especiales de datos personales» con una especial protección.

37. El Capítulo XI, tercero de esta parte, se ocupa de la digitalización de actividades y contratos, una operativa mucho más creativa e innovadora que la estudiada en el Capítulo anterior. Consta de seis apartados. El primero de ellos trata los llamados *smart contracts*, y ha sido elaborado por Manuel Ángel López Sánchez. Este autor expone cómo nació esta posibilidad de implementar la celebración y ejecución de contratos por medios digitales, y los desarrollos posteriores con aplicaciones en muchos ámbitos. Lo que se pone de relieve, acertadamente a nuestro juicio, es tanto su discutible calificación de «contratos» (a menudo, no son sino un reflejo en medios digitales de un contrato celebrado previamente *offline*), como la limitación del supuesto carácter inteligente/*smart* de estas figuras, dado que por lo general no suponen más que ejecuciones automáticas e inflexibles de órdenes programadas en una aplicación informática. En cualquier caso, estos *smart contracts* se rigen por la normativa general de obligaciones y contratos privados, y por la específica de cada modalidad contractual.

38. El segundo apartado de este Capítulo trata la protección del consumidor en el derecho digital, y ha sido redactado por Carmen Pérez Dios. Especial importancia tiene el tratamiento del concepto de «consumidor digital», que supone que todo aquél que actúe en Internet con un propósito ajeno a su actividad profesional o empresarial está protegido como consumidor, aun cuando puedan ser actuaciones dirigidas al mercado. De esta forma, actúan como consumidores los «no profesionales» que juegan póquer *online* «no profesional» regularmente y viven de esa actividad (STJUE 10 diciembre 2020), o utilizan una plataforma que invierte en instrumentos financieros (STJUE 3 octubre 2019), o venden en plataformas digitales bienes usados (STJUE 4 octubre 2018). La protección contractual del consumidor se trata en este apartado y también en el siguiente, relativo al «comercio electrónico», elaborado por Verónica San Julián. Y es que básicamente la regulación del comercio electrónico en la Unión Europea se refiere a la contratación con consumidores, aun-

que ha tenido un efecto reflejo muy relevante en la contratación con todo tipo de sujetos. El apartado sobre comercio electrónico realiza un especial énfasis sobre las Directivas 2019/770 y 2019/771, y su trasposición en nuestro derecho por medio del RDL 7/2021, de 27 de abril. La primera de ellas trata del suministro de contenidos y servicios digitales, y la segunda desarrolla el régimen de la compraventa de bienes físicos, tengan o no componentes digitales accesorios. Especial importancia tiene la regla que considera que estos negocios incluyen el supuesto en que el consumidor no paga un precio, pero sí facilita datos personales «como contraprestación», lo cual introduce indirectamente la admisión de los datos personales como precio o mercancía. Ciertamente no son pocos los casos de contratos de este tipo que se autodenominan «gratuitos», pero en los que el empresario busca obtener datos del cliente, y por eso el legislador se ocupa de ellos, dejando claro además que el tratamiento de esos datos deberá cumplir la normativa de protección de datos personales.

39. El cuarto apartado de este Capítulo versa sobre las actividades financieras y de pago en el marco digital. Ha sido elaborado por María Amparo Salvador (en lo relativo al sistema de pagos digitales) y por Eduardo Valpuesta (el resto de aspectos). Ciertamente la actividad financiera se había digitalizado en muchos aspectos procedimentales ya en el último cuarto del siglo XX, con los sistemas bancarios de saldos digitales y compensación electrónica y los de negociación de valores de interconexión bursátil. Pero las nuevas tecnologías no sólo han mantenido y modernizado estos sistemas, sino que han creado nuevas posibilidades, muestra de lo cual es el *Digital Finance Package* publicado en septiembre de 2020, que proponer regulaciones tanto para tecnologías de registro distribuido como para criptoactivos. En la parte de sistemas de pago se exponen tanto los servicios de pago minoristas como los servicios y sistemas de pago al por mayor, además del régimen jurídico básico de los sujetos que realizan estos servicios. El modelo de inclusión financiera y la generalización de la digitalización de los servicios de pago ha hecho surgir, además, la obligación para las entidades bancarias de ofrecer acceso a cuentas de pago a todos los ciudadanos. A continuación se expone el régimen del dinero electrónico, figura introducida por una Directiva de 2009 que ha tenido poca relevancia práctica, y que actualmente quedará desplazada por otros sistemas más desarrollados y útiles. También se tratan los servicios y entidades ofrecidos por otras entidades financieras no autorizadas como bancos y que se ayudan de técnicas digitales, las llamadas *FinTech*, e incluso la actuación de las grandes plataformas de oferta de bienes y servicios como financiadores, el fenómeno denominado *TechFin*. Y se realiza una especial referencia a la implementación de figuras propias de la economía colaborativa mediante plataformas digitales de pago o financiación, como las llamadas *DeFi*, un conjunto variopinto de aplicaciones para dispositivos móviles que permiten operaciones financieras entre particulares utilizando redes *blockchain*.

40. El concepto y régimen de los criptoactivos supone una parte importante de este capítulo, unos elementos de perfiles borrosos en auge pese a la absoluta falta de seguridad jurídica que les caracteriza actualmente. Este apartado parte de la división entre criptoactivos de pago, de servicios y de inversión, y desarrolla especialmente lo relativo a las criptomonedas, tanto las originales (que no tienen respaldo alguno del emisor) como las figuras más modernas de las *stable coins* y de las inminentes «divisas digitales». La propuesta de regulación comunitaria MiCA, presentada en septiembre de 2020, supone un intento ambicioso de regulación, si bien no queda claro cuál puede ser su eficacia real, que depende además de posibles modificaciones en su tramitación. Se estudian también las emisiones de estos criptoactivos por medio de las llamadas ICOs o STOs (*Initial Coin Offerings* o *Securities Token Offerings*), que tienen un claro paralelismo con la mecánica de la emisión de valores, régimen que además puede que sea aplicable según el tipo de criptoactivo que se emita. Se finaliza con un desarrollo del régimen fiscal de los criptoactivos, dado que aun a falta de normativa jurídico-privada, lo que sí existen son criterios legales y administrativos en cuanto a su tributación.

41. El quinto apartado del Capítulo se refiere a la digitalización de otras áreas contractuales en ámbitos ajenos a la financiación y pago. En materia societaria, en primer lugar, no sólo se han digitalizado los procesos (de constitución o de desarrollo de la actividad de los órganos sociales), sino también la dinámica societaria en sí misma, a través de las llamadas *Decentralised Autonomous Organisations* (DAO). Este aspecto lo trata Patrick O'Malley, que expone este sistema de instrumen-

tación de todas las relaciones intrasocietarias a través de *smart contracts*. Aunque la primera DAO sufrió un traspié importante cuando uno de los integrantes se apoderó de la tercera parte de los fondos, el modelo como tal se ha seguido aplicando. Continúa una breve referencia al uso de plataformas en la negociación privada, a cargo de Eduardo Valpuesta, que desarrolla cómo las plataformas pueden actuar como meros intermediarios o como prestadores de un servicio principal, ejemplificándolo con los casos judiciales de Ü*ber* (prestación de servicios de transporte, por condicionar fuertemente la actuación de los transportistas) y *Airbnb* (prestación de servicios intermediarios, por no interferir la libertad de organización de los anunciadores). Una tercera parte, también redactada por Eduardo Valpuesta, trata diversos supuestos de prestaciones contractuales que se ofertan por medios digitales, como el asesoramiento (*advising*), el alquiler de vehículos por tiempos reducidos (*carsharing*) o la distribución de bienes sin necesidad de constar con un almacenamiento previo de los mismos (*dropshipping*). El mismo autor se encarga de la siguiente parte, referida al transporte, en la que se expone la electronificación de la documentación del transporte, y la existencia de redes *blockchain* que facilitan diversos aspectos de la contratación marítima: mejorar la eficiencia portuaria, operar la intermediación entre los operadores del transporte, monitorizar la situación y estado de la mercancía o programar el cumplimiento automático de ciertas prestaciones objetivables. La exposición continúa con las diversas aplicaciones de técnicas digitales al seguro (el llamado *InsurTech*), expuesta por Joseba Fernández Gaztea y Eduardo Valpuesta. En este ámbito han surgido nuevas plataformas que operan la contratación o el seguimiento del seguro, e incluso se han creado nuevas formas contractuales aseguradoras (seguros «a la carta» y «por diseño», para tiempos o riesgos muy concretos; bonificaciones según la forma de conducción en los seguros de vehículos; asistencia médica mediante *chatbots*, etc.). Los autores desarrollan también cómo ha incidido la tecnología en la ordenación y supervisión administrativa de los nuevos sujetos (comparadores de seguros, neoaseguradoras, plataformas de *crowdinsurance*, etc.). Por último, estos mismos autores desarrollan diversas aplicaciones digitales en materia de uso de energía, que van desde la creación de plataformas que actúan como *marketplaces* para la comercialización de energía, pasando por la facilitación de la *eMobility* o la *tokenización* para la financiación de proyectos de energía renovable, hasta la instauración de redes *blockchain* para la negociación de energía *peer-to-peer*. La tecnología digital puede utilizarse, además, para lograr la trazabilidad de la energía renovable, o crear redes de autoconsumo colaborativo.

42. La última parte de este Capítulo se refiere a la incidencia de la digitalización en las relaciones laborales. Ciertamente la tecnología también ha tenido incidencia en este ámbito, tanto al automatizar ciertos trabajos, cuanto al introducir nuevas tecnologías que varían la forma de prestación de las obligaciones laborales. Esta colaboración sido elaborada por Inmaculada Baviera, que divide su exposición con base en los marcos jurídicos comunitario y español. En cuanto al primero expone las consideraciones realizadas sobre la aplicación de inteligencia artificial en el trabajo, la necesidad de competencias digitales en los trabajadores, la protección de datos personales, la regulación del teletrabajo y el derecho a la desconexión digital, y la mejora de las condiciones laborales de quienes trabajan para plataformas sociales. En cuanto al marco jurídico español, la autora se centra en varios aspectos concretos, de entre los que destacan la protección de la privacidad y la intimidad en el puesto de trabajo, la calificación jurídica de los *riders* (con el reflejo de los criterios recogidos en la nueva disposición adicional 23ª ET, introducida por la Ley 12/2021), y el derecho a la desconexión fuera del horario de trabajo.

43. Cierra esta parte tercera del Tratado un último Capítulo relativo a la cibercriminalidad, que constituye también una manifestación de cómo las técnicas digitales crean nuevas figuras de participación delictiva e incluso nuevos delitos. El estudio de esta materia se divide en tres partes. La primera de ellas, a cargo de Elena Íñigo, trata de los delitos informáticos, y pone de relieve cómo las nuevas tecnologías crean formas distintas de cometer hechos delictivos «clásicos», y también generan nuevos tipos delictivos que no podían ser imaginados por el legislador de hace unos años. La autora distingue los delitos que tienen por objeto bienes informáticos (como los daños y sabotajes a equipos informáticos, o el uso no autorizado de terminales de telecomunicación ajenos) de los delitos que utilizan la informática como medio de comisión (delitos por medios informáticos, que

incluyen tipos de delincuencia económica, o de delincuencia sexual –como el *sexting* o el *cyberbulling*-), y realiza también una referencia al terrorismo practicado en el ciberespacio. Una segunda parte se refiere a la nueva caracterización de la responsabilidad en los delitos cometidos en contextos digitales, y ha sido redactada por Pablo Sánchez-Ostiz. Se trata de aplicar las estructuras lógicas clásicas de la imputación, pero teniendo en cuenta las especialidades que introduce la comisión sobre bienes informáticos o por medios informáticos. Se expone así la determinación de la responsabilidad (persona física que comete el acto delictivo, posibles personas físicas que colaboran para esa comisión, y posible responsabilidad de personas jurídicas en ciertos supuestos) y las consecuencias sancionatorias especiales (como la clausura, destrucción o incautación de los productos informáticos que sean objeto o instrumento del delito). Por último, se trata de la aplicación de técnicas de *big data* e inteligencia artificial en la comisión y prevención de delitos, colaboración que ha sido elaborada por Mario Pereira. Se parte de que actualmente la inteligencia artificial se halla en un estudio muy prematuro de desarrollo, y no sustituye por ahora a la decisión y programación humana. El trabajo expone consideraciones sobre posibles usos de inteligencia artificial para la comisión de delitos, pero también para su investigación. Y finalmente introduce el peligroso tema de la «predictibilidad delictiva», que no solamente puede indicar un «mapa de riesgos», sino incluso asignar el carácter de futuro delincuente a ciertos sujetos. De forma totalmente acertada, el autor desconfía de esa aplicación tecnológica por el manifiesto riesgo de incurrir en tratos discriminatorios y en valoraciones infundadas.

6. Competencia y propiedad intelectual en la sociedad digital

44. La última parte de este *Tratado* trata conjuntamente cómo la sociedad y la economía digitales han supuesto una nueva realidad y planteamiento para la competencia y la propiedad intelectual e industrial. En particular, el «efecto de red» crea un nuevo escenario dentro de la competencia entre las empresas que operan en el mercado digital y de las telecomunicaciones; la operativa por internet origina nuevas formas desleales de competencia; y las nuevas tecnologías cambian por completo la forma en que se puedan reflejar y comercializar las creaciones intelectuales e industriales. Por eso tiene sentido efectuar un repaso general a cómo quedan afectados estos sectores en la economía digital. Esta parte se desarrolla en cuatro capítulos.

45. Se trata en primer lugar cómo opera la defensa de la competencia en los mercados digitales. Este Capítulo ha sido redactado por Carolina Fernández Bustillo, quien parte poniendo de manifiesto la enorme concentración dentro de los mercados digitales, dominados por unas pocas empresas que crean además una situación de «ecosistemas de productos y aplicaciones interoperables» que atrapa al usuario. Esto ha hecho, se continúa razonando, que se cuestione si la competencia debe seguir protegiendo, como se defendía hasta ahora, el interés del consumidor, o debe cambiarse de paradigma para proteger el proceso competitivo y la competencia efectiva en su totalidad, impidiendo la concentración y que valores adicionales como la pluralidad de la oferta, la sostenibilidad, la justicia social o la inclusión sean igualmente defendidos. Se expone igualmente la discusión acerca de cómo determinar el «mercado relevante» en el caso de plataformas que conectan usuarios de varios lados, de forma que podría considerarse a cada uno de los lados como mercado relevante separado (posición de la Unión Europea) o un único mercado de dos lados (posición del TS estadounidense). El Capítulo expone los diferentes supuestos que se han tratado hasta ahora en la jurisprudencia y práctica comunitaria y estadounidense como acuerdos colusorios, abuso de dominio, y autorización de concentraciones, resaltando aspectos tales como la concertación en el uso de algoritmos, la concertación a través de facilitadores (*hub&spoke*), la restricción de ventas pasivas y el geobloqueo, las prohibiciones de venta a través de canales *online*, o las cláusulas de paridad.

46. El segundo Capítulo de esta parte se dedica a la competencia desleal en la sociedad digital, elaborado por Estibaliz Peinado y Borja Sainz de Aja. Tras una exposición general acerca del bien protegido en esta materia –la competencia por eficiencia o competencia por las prestaciones-, se pone de manifiesto la estructura de la Ley, que fija una cláusula general de ilicitud (conductas contrarias a la buena fe objetiva) y luego supuestos concretos de conductas desleales, y por último una «lista negra» de actuaciones desleales con con-

sumidores. A partir de ahí se exponen supuestos concretos de conductas que se han considerados ilícitas dentro de los mercados digitales tanto por infracción de cada una de las reglas de supuestos concretos (actos de engaño, actos de confusión, prácticas agresivas, actos de denigración, actos de comparación, actos de imitación, explotación de la reputación ajena, violación de secretos, inducción a la violación contractual, violación de normas, y discriminación y dependencia económica) como de la cláusula general. Se estudian así supuestos específicos que se producen en estos mercados, como la interacción falseada (*fake engagement*), el *framing*, el empleo de signos distintivos ajenos como *adwords* y el uso indebido de *metatags*, el *cybersquatting*, el *cracking* o el *screen scraping*.

47. El tercer Capítulo de esta parte, redactado por Rafael Sánchez Aristi, se dedica a cómo queda afectada la propiedad intelectual por las nuevas tecnologías digitales. Parte este autor de que la posibilidad de convertir cualquier obra intelectual en información susceptible de ser expresada en código binario, ha permitido almacenarla, procesarla y transmitirla por redes digitales, cambiando por completo las formas de operar clásicas. Surgen, así, desde nuevos objetos de protección (como los programas de ordenador, o las bases de datos electrónicas) hasta nuevos formatos de producción y consumo y nuevas formas de realizar los actos de reproducción, distribución, comunicación pública o transformación. La normativa ha ido intentando acomodarse a los cambios, siendo la última aportación en el ámbito comunitario la realizada por la Directiva 2019/790, sobre los derechos de autor y derechos afines en el mercado único digital, que busca un equilibrio entre los intereses de los creadores y de los usuarios. El Capítulo presta especial atención a los límites o excepciones que amparan la posibilidad de realizar determinadas utilizaciones de una obra o prestación protegida sin necesidad de contar con el permiso del titular de los derechos, y cómo se han adaptado al espacio digital. De acuerdo con ello, se realiza un detallado estudio del régimen de compensación equitativa por copia privada, de la minería de textos y datos, de la ilustración de la enseñanza en un entorno digital transfronterizo, del uso de obras huérfanas y fuera del circuito comercial, y de la agregación de contenidos en línea. Se finaliza con una exposición acerca de cómo se han adaptado los medios de tutela al entorno digital en los ámbitos civil, penal y administrativo.

48. El último Capítulo de esta parte, y de la obra, trata de la propiedad industrial y el derecho digital. Ha sido elaborado por Ingrid Pi i Amorós, Borja Sainz de Aja y Álvaro Seijo Bar. Como ocurre con la propiedad intelectual, también los diversos derechos de exclusiva que en España agrupamos bajo la denominación «propiedad industrial» han sido afectados por las nuevas técnicas de difusión de información y de comercialización que permite Internet. En la parte relativa a los signos distintivos, se realiza primero una exposición general del concepto y régimen de marcas y nombres de dominio, para luego exponer una serie de «grupos de casos» de utilización de marcas en el entorno digital, que pueden ser lícitos en función del cumplimiento de una serie de requisitos. Se trata así el uso de marcas como nombres de dominio, la reproducción de marcas en el entorno digital, el uso de marcas en buscadores, o la problemática del agotamiento del derecho de marca en el ámbito del comercio electrónico. En cuanto a las invenciones de uso industrial, se expone el régimen general del concepto y contenido del derecho de patentes, con especiales referencias a cuestiones específicas digitales, como la patentabilidad de los programas de ordenador que incorporen un efecto técnico más allá de la mera ejecución del programa en la máquina, o las invenciones implementadas mediante programas de ordenador relativas a la inteligencia artificial.

7. Recapitulación

49. En definitiva, nos hallamos ante una obra muy completa y detallada, que intenta abarcar todas las facetas de cómo afecta la sociedad digital al ámbito del derecho bajo un orden sistemático adecuado. El partir de los datos digitales como elemento que da sentido a la regulación constituye un buen punto de partida, ya que todo lo expuesto se refiere a conversión de datos no digitales en digitales y a su uso posterior. Y esa digitalización añade un nuevo medio de expresión y una nueva forma de comunicación y de uso.

50. Contemplamos hoy con enorme tristeza cómo ha cambiado el tipo de sociedad basada en relaciones personales «presenciales» a una nueva forma de comunicación mediante técnicas digitales que invade tanto los ámbitos personales como comerciales. Nos guste o no, esta nueva realidad

se ha implantado, y mientras siga imperando hay que entender cómo adecuar nuestra normativa a estas nuevas maneras de relación. El enorme número de normas hoy en preparación, tanto en la Unión Europea como en otros ámbitos, se encuentra además ante el reto de no suponer un freno a la buena innovación, pero aplicar los límites jurídicos y éticos que son absolutamente necesarios. Esta obra puede servir como un marco general que ayude a comprender mejor este sector del derecho y el conjunto de principios que deben vertebrarlo.