4 La problemática jurídica de la protección de datos en la «Smart mobility». Especial referencia al Reglamento 2016/679

JOSÉ ALBERTO ESPAÑA PÉREZ

Contratado predoctoral en la UMA

ISSN 0210-8461

Revista española de Derecho Administrativo 207
Julio - Septiembre 2020

Sumario:

RESUMEN: *La ciudad inteligente impone un nuevo concepto de movilidad, más respetuoso con el medioambiente y la calidad de vida de los ciudadanos. La llamada smart mobility constituye su principal bastión al aprovechar las ventajas que ofrecen las tecnologías de la información y la comunicación a los desplazamientos. Si bien los principales estudios en la materia se han fijado en los aspectos técnicos de la inteligencia artificial, pocos han reparado en los problemas jurídicos que se derivan de su despliegue, especialmente, los ocasionados por la multitud de datos que precisan las aplicaciones de movilidad para ofrecer sus servicios. Ese es el objetivo de este trabajo: analizar y comprobar la influencia que las innovaciones tecnológicas de la smart mobility tienen sobre el derecho a la protección de datos personales, principalmente en el ámbito de la Administración Pública ya que la misma, dada sus competencias, va a ser receptora de una gran cantidad de información de los ciudadanos. Todo ello, con especial énfasis en el Reglamento europeo de Protección de datos.*

ABSTRACT: *The smart city imposes a new concept of mobility, more respectful of the environment and the quality of life of citizens. The so-called smart mobility constitutes its main bastion by taking advantage of the advantages offered by information technologies and communication when traveling. Although the main studies on the subject have been focused on the technical aspects of artificial intelligence, few have noticed the legal problems that arise from their deployment, especially those caused by the multitude of data required by mobility applications to offer its services. That is the objective of this work: to analyze and verify the influence that the technological innovations of smart mobility have on the right to the protection of personal data, mainly in the field of Public Administration, given its competencies, goes to be a recipient of a large amount of information from citizens and paying attention to the new European Data Protection Regulation.*

PALABRAS CLAVE: *Movilidad inteligente - Ciudad inteligente - Protección de datos*

KEYWORDS: *Smart mobility - Smart city - Data protection*

I. INTRODUCCIÓN

El aumento de la sensibilidad por el medioambiente ha despertado una nueva conciencia social que reclama un mayor respeto hacia la naturaleza y los entornos naturales, que en los últimos años se han visto afectados por la creciente tendencia urbanizadora de la población mundial1). Ante este panorama, numerosas voces alertan de los riesgos que la contaminación y la presencia de gases tóxicos en la atmósfera suponen no sólo ya para los ecosistemas sino también para la salud de las personas2). Frente a esta situación, la denominada *smart mobility* (movilidad inteligente) se ha erigido como un mecanismo apropiado para lograr que los desplazamientos por las ciudades se realicen de manera sostenible y eficaz. Un fenómeno que nace como consecuencia de la aplicación de las Tecnologías de la Información y de las Comunicaciones (TIC) a los desplazamientos de las personas en las ciudades para, de este modo, lograr una mayor eficiencia de las infraestructuras y los servicios urbanos. Así, la inquietud por los problemas medioambientales, las directrices marcadas desde Europa en materia ambiental y la preocupación ciudadana hacia el crecimiento sostenible han provocado que se haya puesto la atención en la inteligencia artificial como una posible solución a los problemas medioambientales.

En efecto, la *smart mobility* engloba numerosas ventajas para construir una ciudad más eficiente desde el punto de vista ambiental y social. Muchas de ellas aún están en pleno desarrollo, pero en un futuro no muy lejano serán una realidad. Entre otras técnicas, supone la expansión de sensores interconectados que aportan información en tiempo real, con lo que se mejoran los servicios urbanos y se les dota de mayor precisión. Como consecuencia, el ciudadano puede desplazarse por la urbe de una manera más cómoda y eficiente. De hecho, la inteligencia artificial se configura como un sistema de gestión y un medio para conservar el entorno y reducir los costes medioambientales de las infraestructuras, además de suponer un avance hacia el control eficiente del tráfico, la explotación de las carreteras y el suministro de información a los conductores3).

Sin embargo, no todos son ventajas. La movilidad inteligente abarca una serie de riesgos y potenciales peligros que a menudo pasan desapercibidos. Así, las diferentes aplicaciones de *smart mobility* operan con multitud de datos personales de sus usuarios para poder ofrecer un servicio lo más individualizado posible. De forma casi “mágica” el ciudadano obtiene una serie de prestaciones personalizadas e intuitivas que les facilita la vida diaria, pero una mala gestión de los mismas o un uso indebido de la información recogida puede desembocar en situaciones poco recomendables que arruinen por completo el despliegue de este fenómeno y socave la confianza de los ciudadanos en este tipo de aplicaciones. Los posibles peligros abarcan desde prácticas poco éticas hasta actuaciones

comerciales abusivas que trasciendan la legalidad4).

Así, la presente investigación se adentra en un tema novedoso para tratar de contribuir al estudio de los actuales procesos de evolución de la movilidad urbana, enmarcado en el ámbito de la ciudad inteligente (*smart city*). Y es que el derecho fundamental a la protección de datos personales es imprescindible en el mundo digital además de configurarse como un pilar de desarrollo social y progreso económico5). A pesar de que existen normas que protegen la privacidad personal, en ocasiones, éstas se vuelven insuficientes ante el panorama cambiante y dinámico en el que se mueve la inteligencia artificial.

En los últimos tiempos, las instituciones públicas han reparado su atención en este aspecto como punto esencial en su discurso en pro de la sostenibilidad. La Administración ocupa un papel esencial en este sentido, dadas sus competencias. La planificación estatal considera este fenómeno como una gran apuesta a medio y largo plazo6). Sin embargo, la distinta naturaleza de los prestadores de los servicios de la nueva movilidad, ya sean públicos o privados, aboca a un complejo panorama desde el ámbito jurídico para la defensa de los derechos del ciudadano. El esperado nuevo Reglamento europeo de Protección de Datos abre una nueva etapa. Fue publicado en el Diario Oficial de la Unión Europea el 4 de mayo de 2016 y es aplicable desde el 25 de mayo de 20187). Sin embargo, aún quedan lagunas que no obtienen una fácil respuesta. Empero, cada vez con mayor asiduidad la doctrina subraya la inadecuada normativa sobre protección de datos frente al mutable escenario donde éstos se mueven y, por ello, exigen la definición de un marco jurídico y ético que normativice el uso de información personal en la era del *big data* para ofrecer mayor seguridad jurídica y respeto a los derechos de los ciudadanos.

Por ello, este artículo pretende ser una primera aproximación al fenómeno de la movilidad inteligente como elemento configurador de la *smart city,* para abordar los problemas jurídicos derivados de su despliegue, especialmente, desde el ámbito de la defensa de los datos personales. Focalizando la atención en la compleja simbiosis entre la utilización de aplicaciones de *smart mobility*, las cuales requieren ingente cantidad de información para operar; y el respeto a esa información recogida que afecta a los derechos de los individuos.

II. «SMART MOBILITY»: UN CONCEPTO EN CONSTRUCCIÓN

Cada vez es más común escuchar el adjetivo *smart* aplicado a multitud de parámetros. En efecto, el término *smart mobility* se ha convertido en habitual en el discurso social, gubernamental y empresarial de los últimos tiempos. Pero pese a su continua utilización no existe un concepto único del mismo. Es una noción relativamente nueva y ligada íntimamente a otro concepto: *smart city*8).

De forma general, con la *smart mobility* se hace referencia a una serie de políticas e iniciativas que pretenden mejorar la movilidad de los ciudadanos por las urbes, ya sea a pie, en bicicleta, automóvil, ciclomotor o transporte público o privado; y todo ello, para reducir costes ambientales, económicos y sociales y haciendo de las innovaciones tecnológicas su principal bastión. Así, se trata de una noción amplia que aborda diversos puntos de vista. No obstante, no existe un concepto único o absoluto del mismo.

En el ámbito normativo, la Unión Europea lleva apostando desde hace tiempo por la ciudad inteligente. De hecho, la considera como “una ciudad que busca abordar las cuestiones públicas a través de soluciones basadas en las TIC sobre la base de una asociación multisectorial, basada en el municipio”9). Pero el organismo supranacional va más allá y propone una metodología específica a la hora de considerar una ciudad como inteligente. La define en función de sus elementos característicos: *smart economy*10), *smart people*11), *smart mobility*12), *smart environment*13), *smart governance*14) y *smart living*15). Esto es, la inteligencia artificial aplicada a la economía, las personas, la movilidad, el entorno natural, la gobernanza y el hábitat. De manera que Europa entiende que una ciudad inteligente lo será cuanto más elementos *smart* contenga. Y dentro de la descripción aportada, se observa como la movilidad inteligente se configura como una característica de la *smart city*, donde la tecnología se pone al servicio del sistema de transporte y logístico de manera integrada y eficaz

A nivel interno, las referencias normativas que aluden al concepto son nulas. Ni siquiera la última planificación del Estado que aborda la movilidad inteligente se pronuncia sobre el concepto16). Ante este vacío normativo, existe una amplia producción doctrinal que se pronuncia sobre el concepto. Los estudiosos consideran que la *smart mobility* es uno de los bastiones de la *smart city*17), y es que “[a] menudo la noción de *smart city* ha sido vinculada a la mejora de las condiciones de movilidad en la ciudad”18). Pese a la importancia que se le reconoce en el ámbito de la ciudad inteligente, no hay consenso entre la doctrina sobre una definición completa que resuma sus características principales y que puedan servir de orientación a las futuras normas en este sentido. Al igual que ocurre con el término *smart city,* el concepto de movilidad inteligente se encuentra en formación y abierto a los sucesivos avances

tecnológicos que se producen.

Aun así, PÉREZ PRADA considera la movilidad inteligente como aquella “que busca ofrecer una red de transporte lo más eficiente, limpia e igualitaria posible para las personas, las mercancías y los datos. Aumenta el potencial de las tecnologías existentes para compartir y proporcionar información a los usuarios, los planificadores y los encargados de la gestión del transporte, permitiendo la modificación y mejora de los modelos de movilidad urbana y los mecanismos de planeamiento (…)”19). La doctrina entiende que los elementos de la *smart mobility* se resumen en: accesibilidad local e internacional, disponibilidad de las infraestructuras TIC, sostenibilidad, seguridad e innovación en el sistema de transporte20). Así, en virtud de las diferentes aproximaciones conceptuales propuestas, los elementos definitorios de la noción podrían resumirse en21):

- La apuesta por una movilidad como servicio, donde la titularidad de los vehículos se sustituye por el concepto de utilización, esto es, la capacidad de adquirir derechos de acceso a los servicios de movilidad.
- Transmisión de datos en tiempo real.
- Infraestructura cada vez más inteligente.
- Fomento del coche eléctrico y del vehículo autónomo.

Pero el concepto *smart mobility* está íntimamente unido a las estrategias de *smart city*. De manera que la noción de movilidad inteligente dependerá de lo que se entienda por el concepto marco de ciudad inteligente, del cual se desprende. No obstante, pese a la falta de consenso en torno al mismo, se pueden resaltar dos elementos recurrentes: sistema eficaz y sistema de movilidad caracterizado por el uso sistemático de las innovaciones tecnológicas22). También existen autores que resaltan los avances tecnológicos en la búsqueda de la eficacia y eficiencia en el sistema de movilidad y otros que se focalizan en el usuario del transporte como consumidor23).

Junto a ello, es preciso destacar que, en ocasiones, es bastante común escuchar hablar del término movilidad sostenible para referirse de manera directa o indirecta a la *smart mobility*. Ambas nociones guardan grandes semejanzas. De hecho, no se entiende una movilidad inteligente que no sea sostenible, aunque es cierto que el término movilidad sostenible goza de mayor tradición en nuestro ordenamiento jurídico. A nivel comunitario, se define la movilidad sostenible como “un sistema y unas pautas de transporte que pueden proporcionar los medios y las oportunidades para conjugar las necesidades económicas, medioambientales y sociales de manera eficiente y equitativa, reduciendo los impactos adversos innecesarios, o evitables, y sus costes asociados, en el tiempo y en el espacio”24). A nivel interno, la propia Estrategia Española de Movilidad Sostenible25) se refiere a ésta como “el conjunto de procesos y acciones orientados a desplazar personas y bienes en el territorio para acceder a las actividades y servicios, con un coste económico razonable y que minimiza los efectos negativos sobre el entorno y la calidad de vida de las personas”26).

Para MARTÍNEZ NIETO la movilidad sostenible “es la que permite satisfacer las necesidades de la libertad de movimientos del presente, con un sistema de transporte integrado que permita la accesibilidad y el desarrollo económico, sin sacrificar otros valores humanos o ecológicos presentes o futuros”27). MELLADO RUIZ considera que “este concepto es mucho más amplio que la actividad de ordenación exclusiva del transporte, superando la visión clásica de regulación del tráfico (motorizado fundamentalmente) y los desplazamientos, para incluir las cuestiones específicas de la planificación y gestión de las diferentes infraestructuras y medios de transportes y movilidad, de accesibilidad a los servicios públicos, de control de la contaminación atmosférica y acústica derivada del uso de vehículos de motor, de ahorro y eficiencia energética en materia de transporte, etc.”28).

En el ámbito administrativo la apuesta por la movilidad sostenible goza de mayor parangón, al menos por el momento. Así, existen numerosos municipios que cuentan con sus planes de movilidad urbana sostenible. Aun así, no existe un concepto único de movilidad sostenible, ni ley proveniente del Estado que regule tal materia29).

En definitiva, ambos conceptos contienen diversos elementos en común. De hecho, no se entiende una movilidad inteligente que no sea sostenible, aunque en el término *smart mobility* la referencia a las tecnologías es indudable. Por ello, en los últimos tiempos el concepto movilidad inteligente está desplazando al de movilidad sostenible, ya que el primero es mucho más amplio, acorde al panorama actual y, en gran medida, porque el adjetivo *smart* ha invadido el día a día.

III. LA «SMART MOBILITY» EN EL SECTOR PÚBLICO

La *smart mobility* se expande con gran avidez pese a ser un fenómeno reciente. Esta nueva forma de entender la movilidad ha generado espacios nuevos donde múltiples relaciones jurídicas subyacentes se dan cita. Por ello, a continuación, se analizará las diferentes posibilidades de la *smart mobility* y los riesgos que ello conlleva. A partir de ahí, se abordará su relevante inclusión en el ámbito de la Administración Pública30).

1. VENTAJAS Y POTENCIALES PELIGROS DE LA MOVILIDAD INTELIGENTE

La tecnología constituye el elemento principal de la movilidad inteligente. Ésta consigue incrementar la eficiencia y sostenibilidad de los servicios relacionados con los desplazamientos en la ciudad. Algunas de las diferentes ventajas son accesibles hoy en día, como, por ejemplo, las aplicaciones desarrolladas por las empresas de transportes públicos que permiten al usuario conocer los tiempos de llegada. Sin embargo, el aspecto más icónico en este sentido son los sistemas de navegación incluido en casi todos los vehículos actuales. Gracias a ellos, el conductor puede visualizar a través de un mapa el punto exacto donde se encuentra, su ruta, trayectos alternativos o paradas de interés. Junto a ello, destaca un hecho crucial en la expansiva tendencia de los sistemas de *smart mobility*: el GPS con el que cuentan los teléfonos móviles. De este modo, se puede saber dónde se halla exactamente una persona o el trayecto que hace habitualmente. Mediante la geolocalización se trazan los patrones de movilidad de la población, se puede identificar las infraestructuras más demandadas o cuáles son las zonas más transitadas31). Pero la aplicación de la tecnología al ámbito de la movilidad es muy amplia. Hay sensores que son capaces de detectar automóviles, ya sean de tipo acústico, radares de microondas, de infrarrojos, dispositivos Bluetooth o etiquetas de identificación de frecuencia por radio32). A la hora de rastrear a los peatones, los sistemas de imagen por vídeo pueden realizar conteos a través de las cámaras33).

En los últimos tiempos se ha vuelto frecuente que los medios de desplazamientos públicos distribuyan tarjetas inteligentes para usar sus servicios34). Éstas reportan una gran información sobre los patrones de movilidad de las personas que las utilizan, además, de revelar el medio más usado, los trasbordos realizados, la duración del trayecto, la parada de origen y de destino, etc.35)

Diferentes ejemplos que muestran como la llegada de la *smart mobility* se ofrece altamente ventajosa. Con ello, se puede conocer en tiempo real la información del tráfico y los viajes, mejorar la gestión del transporte público y de mercancías, la gestión de las carreteras y de los aparcamientos36). Pero todo este sistema se articula bajo un elemento clave: los datos. Gracias a ellos las aplicaciones de movilidad inteligente se vuelven altamente eficaces y pueden proporcionar un servicio individualizado. Como afirma RODRÍGUEZ BUSTAMANTE, “[p]ara que la estrategia de movilidad en una ciudad sea lo más «smart» posible […] resulta fundamental contar con datos abiertos que nos faciliten el análisis de la información de cara a la planificación urbana y la movilidad en la ciudad”37). Para que la *smart mobility* sea una realidad es preciso que el usuario ceda ingentes cantidades de información personal que acaba en masivas bases de datos que operan bajo parámetros técnicos e informáticos. A todo ello se une que los movimientos de las personas son repetitivos y predecibles y, por tanto, pueden llegar a ser identificadores de ciudadanos concretos a pesar de que se intenten anonimizarlos38).

Este complejo panorama ha provocado que surjan voces que alerten de los graves riesgos que conlleva el despliegue de la inteligencia artificial a los sistemas de transportes, desde una menor intimidad, falta de seguridad en la protección de los datos o hasta un mayor poder del Estado en la vida privada de los ciudadanos39). Así, un panorama poco aconsejable podría desembocar en gobiernos que rastreen los movimientos de las personas, sus costumbres y preferencias; o en empresas que abusen de la información recogida para desplegar prácticas comerciales abusivas o en contra de la libre competencia, así como el desarrollo de actividades de *profiling*40) que trasciendan los límites legales41). Por no mencionar los problemas derivados de la seguridad de los sistemas de almacenamiento de los datos42). Dentro del sector público son especialmente importantes los riesgos derivados de las fugas de datos que podrían desembocar en ataques informáticos que atentaran contra los derechos de miles de ciudadanos simultáneamente.

Igualmente, la Administración Pública se ve totalmente revolucionada por esta nueva forma de proceder. Ella, dada sus competencias en transportes y movilidad, va a ser receptora de una gran cantidad de información personal de los ciudadanos. Además, esos datos no solo van a ser utilizados por la Administración que ofrezca servicios de desplazamientos, sino también por empresas privadas que presten los mismos y que operen con el sector público. Esto aumenta, aún más si cabe, los peligros.

En definitiva, el tratamiento masivo de la información personal conlleva un nuevo escenario que proporciona ventajas y riesgos a partes iguales. Los datos se han convertido en el petróleo de nuestro siglo, sirviendo como mercancía con la que operan los servicios digitales y haciendo creer al consumidor que los mismos no tienen ningún coste para

ellos. Consecuentemente, se hace necesario tomar en consideración este nuevo panorama y establecer mecanismos que protejan y velen por los derechos de los ciudadanos para que éstos no vean mermada su posición jurídica en la sociedad digital.

2. LAS MÚLTIPLES RELACIONES JURÍDICAS DE LA MOVILIDAD INTELIGENTE

Las estrategias de movilidad inteligente involucran a un gran número de agentes dada las diferentes relaciones jurídicas que subyacen. En primer lugar, nos encontramos con la Administración Pública. Al ofrecer los servicios de movilidad inteligente va a ser receptora de un volumen considerable de información de los usuarios, además, de la que ya posee43). Todo esto debe conjugarse con los principios de transparencia y buen gobierno para evitar abusos frente a la recopilación masiva de datos.

La Administración, por regla general, no precisa del consentimiento de los titulares de los datos cuando éstos se recogen en el ámbito de sus competencias, siempre y cuando su uso sea conforme a la legalidad, ajustado a derecho y la información que se va a utilizar sea proporcional. Para VALERO TORRIJOS “el hecho de que resulte preceptiva la utilización de la información para prestar el servicio y no sea necesario el consentimiento de aquéllas no permite considerar que cualquier uso de los datos proporcionados o, en su caso, obtenidos sin su consentimiento pueda ser admisible”44). Así, esa falta de consentimiento en el ámbito de la Administración Pública no puede aplicarse a actividades que tengan como objetivo la explotación comercial de los datos personales.

Sin embargo, el sector público puede recurrir al ámbito privado para prestar servicios relacionados con la movilidad inteligente. Es más, dado el total protagonismo y avance de las empresas en la *smart mobility* va a ser más que habitual la omnipresencia del sector privado en este sentido. En tal caso, se estaría ante una cesión de datos, un acceso a los datos por cuenta de terceros. “En consecuencia, a falta de consentimiento por parte de los ciudadanos afectados, sólo cabría admitir que los tratamientos de información tuviesen lugar de forma anónima y conforme a estándares tecnológicos adecuados, exigencias que han de trasladarse también a las condiciones jurídicas en que podrá tener lugar el uso de los datos de los ciudadanos para garantizar la integridad de su derecho fundamental”45). Frente al avance imparable de las empresas tecnológicas se hace fundamental que las Administraciones Públicas adicionen garantías para preservar la intimidad de los ciudadanos frente al imparable avance del sector privado en el fenómeno de la *smart mobility*.

Hasta el momento, nuestro ordenamiento jurídico ha articulado el sistema de protección de datos personales en el consentimiento. El uso de la información personal requiere la aceptación del individuo de manera libre e inequívoca. No obstante, cada vez más se está poniendo en entredicho este elemento frente al imparable avance del *big data*46). Y es que, en ocasiones, el usuario no quiere quedarse al margen de las diferentes posibilidades que le ofrece la inteligencia artificial y se ve abocado a aceptar un sinfín de condiciones sin ni siquiera haber reparado en ellas y quedando, por tanto, la garantía del consentimiento mermada. OLIVER-LALANA y MUÑOZ consideran que el consentimiento es un medio inadecuado para proteger al usuario debido a que por falta de tiempo y capacidad no puede tener un conocimiento adecuado sobre el tratamiento de sus datos. Y en caso de no prestar el mismo, queda excluido de la sociedad de la información47).

Es cierto, que la mayoría de los usuarios renuncian a leer una amalgama de previsiones sobre el tratamiento de sus datos que llegan a ser incomprensibles para el ciudadano medio. A esto se une que en el ámbito de la movilidad inteligente las cesiones de datos es tónica habitual que implica a su vez la interconexión entre varios actores que operan con la automaticidad y un masivo número de operaciones. En este sentido, el propio Gobierno de España ya alerta que “el consentimiento o la habilitación legal resultan insuficientes y es preciso reconfigurarlas”48).

A su vez, la posibilidad de reutilizar la información personal en el ámbito administrativo dificulta el panorama de la protección de datos personales en las estrategias de movilidad inteligente. “Asimismo, por lo que se refiere al acceso con fines de reutilización, según establece el artículo 2 de la LRISP [Ley sobre reutilización de la información del sector público], sus previsiones sólo se aplicarían a las entidades del sector público, lo que nos llevaría a la conclusión de que no existe obligación legal por lo que se refiere a los sujetos privados, aun cuando estuviesen vinculados a las Administraciones Públicas”49). CANTO LÓPEZ añade que “[...]la relación jurídica entre la Administración pública con los usuarios y con los prestadores de servicios, por un lado, y con los proveedores de servicios de telecomunicaciones, por otro, hace necesario que exista conexión entre ambos sujetos privados con la administración”50).

En cuanto a los actores privados nos hallamos con un amplio número de intervinientes: empresas que prestan un servicio de interés general, empresas que desarrollan aplicaciones inteligentes, entidades que gestionan redes de

telecomunicaciones, etc. En este sentido, tiene importancia los responsables de las bases de datos, que pueden ser la propia Administración o bien se puede recurrir a un tercero. En este último caso, la información recogida es custodiada por un agente privado o, más bien, depositada en la nube. Esto demuestra que las variadas relaciones que se suceden entre los usuarios y prestadores desdibujan los límites establecidos debido a la interconexión que posibilita el *big data*. Junto a ello, hay que tener en cuenta a los prestadores de servicios que permiten el acceso a las redes. Como sostiene VALERO TORRIJOS "[...]su relación jurídica con los usuarios a los efectos de la prestación de servicios públicos no puede confundirse con la que, en su caso, les corresponde como proveedores de servicios de telecomunicaciones dirigidos a los consumidores. Esta dualidad, como resulte evidente, les impide utilizar los datos que obtengan por ambas vías para hacer un tratamiento basado en la conexión de ambas fuentes"51).

Algunos autores proponen plataformas federadas, esto es, "[...] diferentes plataformas, que pueden estar orientadas a diferentes servicios finales para los ciudadanos, intercambian entre sí datos y capacidades de gestión, que estarán distribuidas en diferentes Plataformas pero que serán accesibles desde otras Plataformas diferentes [...]"52). Y COTINO HUESO opta por diferenciar el tratamiento jurídico de la actividad del procesamiento de datos cuando sea realizado por poderes públicos o por el sector privado. "El marco jurídico puede ser diferente a partir de responsabilidad del estado, principio de legalidad, interés público, frente a la libertad de empresa y derechos en juego por el sector empresarial"53).

Por último, no podemos olvidar al receptor de este tipo de iniciativas: los ciudadanos. Ellos son los protagonistas en la *smart city*, receptores de las políticas inteligentes y afectados por la recopilación masiva de datos. En ocasiones se tiende a dejarlos relegados a un segundo plano o se les minimiza frente a complejos algoritmos y tecnologías, pero en la *smart mobility* el ciudadano goza de un papel fundamental donde la posición jurídica de la que goza no puede quedar mermada54).

En definitiva, en el ámbito de la movilidad inteligente nos hallamos con diferentes sujetos intervinientes. La Administración Pública en el ejercicio de sus competencias. Las entidades privadas que prestan servicios de interés general. Las empresas que gestionan las redes de telecomunicaciones. Y los destinatarios de estos servicios, los ciudadanos, cuyos datos se recopilan y acaban bajo el poder del sector público o de terceros55). Así, se dan cita una pluralidad de intereses, tanto públicos como privados, que pueden llegar a ser contrapuestos y generar tensiones y contrariedades.

3. CICLO DE VIDA DE LOS DATOS EN LA ADMINISTRACIÓN PÚBLICA

En los proyectos de movilidad inteligente están presentes multitud de servicios de naturaleza heterogénea, en especial, servicios de carácter privado cuyas propias particularidades generan numerosos riesgos en el ámbito de los derechos ciudadanos. Así, nos encontramos con empresas que prestan servicios pertenecientes a sectores liberalizados (como por ejemplo la energía) que provoca que una pluralidad de prestadores privados ofrezca dichos servicios. Los potenciales peligros son extensos, ya que los datos que pueden proporcionar no son genéricos, sino que se hallan fragmentados en tanto en cuanto afectan a un sector de la población radicado en un lugar concreto. Esto puede provocar que se realicen perfiles poblacionales, así como conocer datos precisos de los habitantes de una zona.

En sentido contrario nos encontramos con los servicios públicos cuya titularidad descansa en la Administración (como es el caso del transporte colectivo urbano), siendo ésta la que presta el servicio a través de los medios legalmente establecidos y, por lo tanto, teniendo todo el poder de control y decisión. No obstante, también puede optar por la gestión indirecta recurriendo a una entidad privada, aunque la Administración seguiría conservando la titularidad del mismo.

En cualquier caso, los datos se convierten en el oro de las diferentes iniciativas *smart*. Por ello, a continuación, nos centramos en el ciclo de vida que tiene la información recopilada por las aplicaciones de movilidad inteligente en el ámbito público.

3.1. Recogida, consentimiento e información

Para proceder a la recogida de información personal de los usuarios, tal y como establece nuestra Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), se debe recabar el consentimiento libre, inequívoco, específico e informado del afectado mediante una manifestación que muestre su voluntad de consentir, según se especifica en el artículo 6 de la mencionada norma. Si ese consentimiento se

pretende efectuar para una pluralidad de finalidades, esté deberá otorgarse para todas ellas (art. 6.2.). El consentimiento tácito, basado en la inacción de los afectados, no es válido.

Eso sí, existen ciertas excepciones a este consentimiento. Cuando los datos personales tengan como finalidad cumplir con una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, el consentimiento no será necesario, según se especifica en el artículo 8 de la LOPDGDD y el artículo 6.1 del Reglamento europeo de Protección de Datos (RGPD). Así, por norma general en el ámbito de la Administración Pública no será necesario recabar el consentimiento del administrado siempre y cuando se vayan a realizar las funciones propias de la Administración y éstas se enmarquen en las competencias establecidas para la misma. Por su lado, cuando los datos recogidos por la Administración supongan proporcionar un valor añadido56), será necesario obtener el consentimiento de los usuarios. Éste debe tener la posibilidad de consentir por separado cada servicio de valor añadido.

Esta posición privilegiada que ostenta la Administración Pública no significa que caiga el requisito de la información, el cual, se mantiene inalterable (art. 11 LOPDGDD y art. 6 del Reglamento europeo de Protección de Datos)57). Como mínimo, el usuario debe conocer la identidad del responsable del tratamiento, la finalidad y la posibilidad de ejercer sus derechos legales.

Algo muy común en las aplicaciones de movilidad inteligente es la elaboración de perfiles a través de los datos obtenidos de los usuarios para ofrecer unos servicios más personalizados. Una técnica especialmente peligrosa ya que a través de los patrones de movilidad de los usuarios se pueden conocer rutinas, lugar de trabajo o el domicilio de una persona. Esta posibilidad también es contemplada por la norma europea y, por consiguiente, por la ley española; estableciéndose la obligación de informar al usuario de tal situación, pudiendo éste oponerse58).

La Ley también detalla el conjunto de derechos que le asisten al afectado, esto es, los comprendidos en los artículos 15 a 22 del Reglamento europeo de Protección de Datos. Y que se concretan en el derecho de acceso (art.13 LOPDGDD), rectificación (art.14 LOPDGDD), supresión (art. 15 LOPDGDD), limitación del tratamiento (art.16 LOPDGDD), a la portabilidad (art. 17 LOPDGDD) y de oposición (art. 18 LOPDGDD).

3.2. Tratamiento

La normativa de protección de datos establece la necesidad de tener un responsable del tratamiento que recaerá en quien “ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas” (art. 28.1 RGPD). A su vez, se impone una serie de obligaciones al responsable y encargado del tratamiento, teniendo presente algunos riesgos especialmente sensibles a la hora de trabajar con datos personales. Todos ellos, muy comunes en las aplicaciones que operan con la inteligencia artificial como pueden ser los mencionados perfiles personales mediante su localización o sus movimientos o el tratamiento masivo que implique a un gran número de afectados (art.28.2 LOPDGDD)59).

En el ámbito del sector público se podrán atribuir competencias propias de un encargado del tratamiento a un órgano administrativo mediante una norma reguladora y cumpliendo con las exigencias del Reglamento europeo de Protección de Datos (art.33.5 LOPDGDD). Además, los datos personales recogidos podrán almacenarse en servidores propios o ajenos. En el caso que los responsables del tratamiento traten y almacenen datos personales en sus propios servidores, la Administración responsable deberá comprobar que los niveles de seguridad ofrecidos son equivalentes a los suyos y que los datos se devuelven o destruyen cuando acaba el contrato. En este sentido, el texto europeo prohíbe a los encargados delegar sus funciones en otros, a no ser que medie “autorización previa por escrito, específica o general, del responsable” (art. 28.2 RGPD). Como afirma NÚÑEZ GARCÍA tal precepto parece evocar la figura del contrato en nombre y por cuenta de tercero (asimilable al artículo 1.259 del Código Civil español) más que a una subcontratación, ya que es necesario un consentimiento por escrito60). El propio Reglamento europeo parte de la libertad formal, pero establece una serie de detalles que debe reunir el mencionado negocio jurídico (art. 28.3 RGPD). Pero ello no exime de responsabilidad al encargado primigenio, ya que en caso de incumplimiento por parte del subencargado, “el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado” (art. 28.4 RGPD).

Asimismo, en función del nivel de riesgo del tratamiento de los datos se pueden distinguir tres escalas de obligaciones. Tal y como establece LÓPEZ ÁLVAREZ la Administración Pública se encuentra en el tercer grupo “pues su obligación no deriva del tamaño de la organización, sino de que el tratamiento que realice incurra en alguna de las siguientes circunstancias: que entrañe un riesgo para los derechos y libertades de los interesados, no sea

ocasional, incluya categorías especiales de datos personales cuyo tratamiento esté prohibido, o incluya datos personales relativos a condenas e infracciones penales, o a medidas de seguridad conexos"61).

No obstante, dentro de la Administración Pública debe estar presente la filosofía del *open data,* de manera que la información no puede almacenarse de forma estanca, sino que debe cumplir con los criterios de apertura y accesibilidad. Pero para acatar los estándares que propugna el *open data* es necesario una gestión documental que cumpla con los parámetros de interoperabilidad, esto es, que la información se encuentre en versión electrónica y se garantice la accesibilidad y la interconexión, siempre que se respeten las medidas de seguridad dispuestas al efecto. Ello conecta con las estipulaciones de la Ley de transparencia, acceso a la información pública y buen gobierno. Aunque en muchas ocasiones la propia Administración Pública se escuda en la Ley de protección de datos para no cumplir con los preceptos de la Ley de transparencia, lo cierto es que ésta es título habilitante para esclarecer si se debe dar acceso a la información pública que poseen los obligados por la misma. RAMS RAMOS afirma que "[e]s pues, el órgano o entidad que posee la información quien debe decidir, a través del procedimiento de acceso a la información previsto en los artículos 17 y siguiente LTBG [...]"62).

3.3. Uso

En cuanto a la utilización de los datos recogidos, éstos deberán limitarse al fin establecido, evitando injerencias sobre la privacidad del usuario. Así, debemos recordar que la Sentencia del Tribunal Constitucional 291/2000 (RTC 2000, 291) considera que el derecho a la protección de datos abarca un poder de disposición y de control sobre la información personal que faculta a la persona para decidir cuáles de esos datos se da a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y posibilita al individuo a saber quién tiene esos datos personales y para qué, pudiendo oponerse a esa posesión o su uso63).

Sin embargo, en el ámbito de la Administración Pública donde se emplean tratamientos automatizados de los datos no se puede perder de vista las dificultades jurídicas que impone la normativa sobre acceso y reutilización de la información64). Por este motivo, CANTO LÓPEZ propone separar los datos a partir de la información con relevancia y no de los documentos para respetar derechos como la intimidad, la seguridad pública o los datos personales65).

3.4. Cesión de datos a otras administraciones

La cesión de datos a otras administraciones debe ser consentida o basada en una norma habilitante. El artículo 6 del Reglamento General de Protección de Datos legitima para la utilización de los datos personales y la cesión de los mismos por parte de las Administraciones Públicas. En efecto, se permitirá cuando el tratamiento sea necesario para cumplir con una obligación legal aplicable al responsable del tratamiento y cuando éste sea destinado a cumplir con una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. La LOPDGDD en su artículo 8 recalca cuándo el tratamiento de datos personales podrá entenderse fundado en el cumplimiento de una obligación legal exigible al responsable en los términos del artículo 6. c) del Reglamento europeo. Esto es, cuando lo establezca una norma de Derecho de la Unión Europea o una norma con rango de ley, que determine las condiciones generales del tratamiento y los tipos de datos a tratar, así como las cesiones. Aunque VALERO TORRIJOS alerta que los controles de la cesión de datos son inadecuados, siendo conveniente abordar unas garantías para la tutela de los bienes jurídicos presentes, tanto públicos como privados66).

3.5. Cancelación y destrucción

El ciclo de vida de los datos personales finaliza con su pertinente cancelación o destrucción. Cuando dejen de ser necesarios al fin para el cual se recogieron el responsable deberá cancelarlos o eliminarlos por completo (art. 33.3 LOPDGDD). La cancelación será pertinente cuando el usuario cause baja. De forma que los datos estarán bloqueados, impidiendo su tratamiento, e incluso su visualización (art. 32 LOPDGDD).

En este sentido, es preciso tener en consideración la protección de datos de los difuntos, cuestión introducida por la nueva normativa. El artículo 3 de la LOPDGDD contempla que las personas allegadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento para solicitar el acceso a los datos personales de aquel y proceder a la rectificación o supresión. Ahora bien, los sujetos anteriormente mencionados, no podrán acceder a los datos del difunto, ni pedir su rectificación o supresión, cuando el causante lo hubiese prohibido expresamente o así se establezca por ley. El fallecido podrá designar expresamente a personas o instituciones para solicitar el acceso a los datos personales de éste y pedir su rectificación o eliminación, según las instrucciones dadas.

4. LA SALVAGUARDIA DE LOS DATOS PERSONALES EN LA MOVILIDAD INTELIGENTE. ESPECIAL REFERENCIA AL REGLAMENTO EUROPEO 2016/679

La gestión de la movilidad inteligente cambia la perspectiva tradicional por una nueva marcada por la tecnología y las nuevas formas de operar digitalmente. Las TIC posibilitan el aumento de la demanda de transporte multimodal, de nuevos modos de transporte privados, así como el control de la circulación, geolocalización de los usuarios de las vías y un largo etcétera. Pero para conseguir todo esto se necesita recopilar multitud de datos personales de los ciudadanos.

Con esa recopilación de datos se viabilizaría, por ejemplo, la identificación de vehículos particulares para establecer en tiempo real rutas no congestionadas o el control de los semáforos. En este dinámico escenario la mirada de los juristas se vuelve a la protección del derecho a la intimidad o la preservación de la privacidad en los servicios de movilidad inteligente disponibles en la ciudad67).

En este sentido, se precisa una respuesta por parte del Derecho que sea capaz de garantizar la salvaguarda de los derechos fundamentales de los ciudadanos, sin embargo, la velocidad de los cambios provoca que éste se vea incapaz de ofrecer una adecuada seguridad jurídica68). Así, es preciso tomar en consideración el Reglamento General de Protección de Datos que deroga la anterior Directiva 95/46/CE, la cual, se había quedado obsoleta frente al avance tecnológico69). En consonancia con el Reglamento, también destaca la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, modificada por la Directiva 2009/136/CE, que insta a los Estados miembros a velar por los derechos de las personas físicas en relación con el tratamiento de los datos personas y el derecho a la intimidad. No obstante, desde que el texto vio la luz los cambios en el entorno digital se han sucedido de manera vertiginosa y el desarrollo de las aplicaciones de movilidad inteligente es un fenómeno reciente. Por ello, se hace necesario adaptarlo a la nueva realidad y tomar en consideración aspectos que no se tuvieron en cuenta. En este sentido, la Comisión Europea presentó en enero de 2017 la Propuesta de Reglamento sobre privacidad de las comunicaciones electrónicas, que derogaría la Directiva 2002/58/CE, y que pretende aumentar los niveles de protección de la privacidad de los ciudadanos de la Unión Europea. Igualmente, el legislador europeo ha decidido cambiar dicha directiva por un reglamento para lograr una mayor armonización entre los Estados miembros. Sin embargo, dado que no se trata de normativa vigente, centraremos nuestra atención sobre el Reglamento General de Protección de Datos.

En este sentido, el Reglamento no solo tiene por objetivo que el tratamiento de datos no viole los derechos fundamentales, sino que entiende que el hecho de tratar datos personales puede violar la protección de los mismos, de ahí, que se apueste por ofrecer un adecuado marco jurídico que proporcione seguridad jurídica70). A nivel europeo se entiende por dato personal toda información sobre una persona física identificada o identificable. Es decir, “toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador de línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona” (art. 4). Además, hay una serie de datos especiales que gozan de un tratamiento diferenciado, y son aquellos que aluden al origen racial o étnico, la ideología política, las convicciones religiosas o filosóficas, la afiliación sindical o datos relativos a la salud o la vida sexual de una persona (art. 9). Igualmente, por tratamiento de datos se entiende “cualquier operación o conjunto de operaciones, realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción” (art. 4). Los datos serán recopilados por la autoridad competente con un fin determinado, explícito y legítimo, y solo podrán ser utilizados para el fin previsto.

El Reglamento establece la obligación de elaborar una evaluación de impacto en la privacidad (art. 3). De modo que cuando se presuma que un tratamiento implica un alto riesgo para los derechos y libertades de las personas, los Estados miembros dispondrán que el responsable de los mismos lleve a cabo, previamente, una evaluación del impacto de las operaciones de tratamiento previstas.

Además, se establecen los requisitos que debe reunir el consentimiento para que el tratamiento sea lícito (art. 7). Se exige que el responsable sea “capaz de demostrar que aquél (el interesado) consintió el tratamiento de sus datos personales”. Aunque el consentimiento puede ser tácito, salvo en datos de especial protección (algo común en las aplicaciones inteligentes que recaban datos); a la hora de probar su existencia los mecanismos se refuerzan, ya que no basta con la simple falta de actividad del usuario71).

El nuevo Reglamento también regula los derechos que tienen los sujetos de los que se obtienen los datos, los cuales, se pueden resumir en el derecho a la información y el derecho a oponerse. Así, se encuentra el deber de ser informado sobre la recopilación o tratamiento de datos personales por las autoridades competentes, según el Derecho nacional72). Pero ese deber de información debe hacerse de "forma concisa, transparente, inteligible y de fácil acceso" (artículo 12), de manera, que el legislador europeo consciente de que en muchas ocasiones la información que se ofrece es bastante compleja y llena de aspectos técnicos, establece la obligatoriedad de proporcionar una información asequible al ciudadano medio. De otro modo, el consentimiento no sería válido ya que se entendería que el usuario no ha comprendido para consentir. Y, junto a ello, el derecho de acceso a los datos, es decir, la capacidad que tiene el sujeto de tener conocimiento sobre la información suya que ha sido recopilada, así como sus destinatarios a los cuales se les han remitido esa información. Sin embargo, éste no es un derecho absoluto, sino que encuentra limitaciones en la necesidad de evitar que se obstaculicen investigaciones; procedimientos judiciales; protección de la seguridad pública, la seguridad nacional o los derechos y libertades de terceros, entre otras limitaciones (art. 15). También se localiza el derecho de rectificación, supresión o bloqueo en los términos que aparecen recogido en la mencionada norma (art. 16 y 17). Los Estados miembros son los encargados de decidir si el derecho se ejerce de forma directa o a través de la autoridad nacional competente. En caso de que el responsable del tratamiento deniegue la rectificación o supresión de los datos personales, éste deberá informar con el razonamiento. Junto a ello se ha introducido el denominado derecho al olvido como consecuencia del pronunciamiento del TJUE que reconoció tal facultad (aunque tal derecho existía con la anterior regulación desde que se dictó sentencia en tal sentido).

Especial importancia en el ámbito de la inteligencia artificial tiene lo establecido en el artículo 22 que regula la elaboración de perfiles. El texto no lo prohíbe ni lo limita, sino que establece ciertas garantías como son "el derecho a obtener intervención humana", a "expresar su punto de vista" (el del usuario) y a "impugnar la decisión". Además, el Reglamento exige a los Estados miembros que adopten las medidas técnicas y de organización para proteger los datos de su destrucción o acceso no autorizado, máxime cuando el tratamiento o transferencia se haga dentro de una red o mediante acceso automatizado directo. En caso de tratamiento automatizado de datos cada Estado miembro deberá exigir al responsable del tratamiento la adopción de una serie de medidas (art.. 29).

En las aplicaciones de movilidad inteligente los datos circulan sin ningún tipo de barrera. En relación con ese flujo transfronterizo de información entre países de la Unión y fuera de ésta, el Reglamento señala una autoridad principal localizada en el Estado donde el responsable del tratamiento tiene su establecimiento principal (art. 56) y una autoridad interesada que interviene porque se afecta a un residente en su territorio (art. 4.22). La norma europea señala una serie de obligaciones que tienen las autoridades de control (arts. 60 y ss.).

Así, las principales limitaciones a la tecnología inteligente para garantizar la privacidad se localizan de manera genérica en el mencionado Reglamento europeo. Una vez resaltado los elementos más significativos y novedosos que contempla el texto abordaremos los aspectos más controvertidos de las aplicaciones de movilidad inteligente bajo el enfoque europeo.

4.1. Seudonimización de los datos personales

Frente a la recopilación de datos por las aplicaciones tecnológicas, algunos autores plantean el empleo de datos anónimos como medida de solución de cara a las posibles intromisiones en la privacidad de los usuarios. Esto es, una vez captados los datos se anonimizan y se olvida el origen de los mismos. De hecho, la Directiva 2010/40/UE que regula los Sistemas Transportes Inteligentes llama al anonimato "como uno de los principios de mejora de la privacidad de las personas"73). A su vez, la Directiva sobre la privacidad y las comunicaciones electrónicas señala que los datos de localización de "los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido". En este sentido, el vigente Reglamento General de Protección de Datos opta por el concepto de seudonimización74) y lo define como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"75). Para algunos autores esta medida pretende "reducir los riesgos para los interesados y facilitar el cumplimiento de la normativa para los responsables y encargados"76).

El Supervisor Europeo de Protección de Datos (SEPD) se ha referido a este término y ha considerado que debe existir una definición clara y vinculante de dato seudonimizado, diferente a la de dato personal, para que éstos no se

enmarquen en el ámbito de protección de las normas defensoras de los datos77). En el Reglamento, los datos seudonimizados aluden a los de una persona física y quedan sometidos a la normativa sobre protección de datos. Con respecto a la información adicional que pueden hacer identificables a un sujeto, el Reglamento destaca los identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos78). El hecho es que las aplicaciones de movilidad inteligente recaban una multitud de datos de sus usuarios, esto unido al *big data* y a la minería de datos, conducen a que, aunque la información se trate de forma anónima se puede llegar fácilmente a identificar la misma con un individuo concreto. De ahí el potencial peligro de esta cuestión.

Para determinar "si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tener en cuenta todos los factores objetivos, como los costes y el tiempo necesario para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos"79). Así, las normas de protección de datos no serían de aplicación a la información anónima, a aquella que no tiene relación con una persona identificada o identificable. Eso sí, los datos deben ser disociados de la forma correcta si no la normativa sobre protección de datos se aplicará a todos los tratamientos de datos personales que se lleven a cabo80).

En este sentido, destaca la Sentencia del Tribunal Superior de Justicia de la Unión Europea de 16 de abril de 2015 (TJCE 2015, 161)81). Dicha resolución analiza el alcance de las bases de datos que contienen información biométrica y el tratamiento de ésta82). En esta ocasión, la duda se centraba en determinar el ámbito de aplicación del Reglamento europeo 2252/200483), en concreto, para el documento de identidad neerlandés. El caso es que varios ciudadanos de los Países Bajos presentaron por separado unas solicitudes de pasaportes y de documento de identidad, que fueron denegados por negarse los interesados a facilitar sus impresiones dactilares. Éstos no quisieron proporcionar sus datos biométricos alegando que la recogida y almacenamiento de los mismos constituye una violación de su integridad física y de su derecho a la protección de su vida privada. El Tribunal concluye que en este asunto no es de aplicación el Reglamento europeo mencionado ya que es competencia de los correspondientes Estados miembros establecer las determinaciones de los requisitos exigibles a sus ciudadanos para expedir la identificación nacional, sin perjuicio de que éstos tengan validez en el ámbito de la Unión Europea cuando una persona se desplaza a otro país miembro. Aunque el caso analizado en esta sentencia no se refiere por completo al despliegue de las tecnologías inteligentes en el campo de la movilidad, resulta especialmente interesante en este sector, ya que los avances técnicos en el ámbito de la *smart mobility* requieren y requerirán con mayor frecuencia de mecanismos de identificación personal para ofrecer servicios personificados al ciudadano.

A nivel interno, la vigente Ley Orgánica de Protección de Datos no se pronuncia al respecto. Aunque la anterior norma en la materia, la Ley Orgánica 15/1999, se refería al procedimiento de disociación como todo tratamiento de datos personales donde "la información que se obtenga no pueda asociarse a persona identificada o identificable", aunque no se extiende más en la cuestión. No obstante, el problema intrínseco a este procedimiento surge respecto a la cuestión de si es posible un procedimiento de anonimato de los datos personales de una persona física donde no sea posible asociar los datos con un sujeto84). Y es que las aplicaciones inteligentes de movilidad recaban tantos datos de sus usuarios, que, aunque sean anónimos, se convierte en algo fácil trazar los mismos para averiguar el individuo que está tras ellos. Respecto a esta cuestión, la doctrina muestra recelos ya que dejaría la puerta abierta a posibles situaciones fraudulentas o una menor especialización de los servicios85).

4.2. Geolocalización

La gran mayoría de las herramientas de movilidad inteligente se basan en la geolocalización, ya que se requiere que el proveedor de servicios conozca la ubicación del usuario para poder operar más eficazmente. Por ello, resulta conveniente hacer breve mención a este aspecto que produce ventajas y riesgos a partes iguales. Su presencia en los teléfonos móviles inteligentes es total y se presta para servicios de mapas y navegación, zonas de interés próximo, historial de ubicaciones o rastreo de paraderos de personas. Para más inri, las aplicaciones que usan la geolocalización pueden utilizar tanto la ubicación actual del usuario como su historial de ubicaciones. La ubicación se puede saber a través del GPS, antenas de redes móviles, dirección IP o señal Wi-Fi. Como consecuencia, su valor es fundamental porque a través de la localización geográfica se pueden averiguar datos financieros, de salud o sobre el comportamiento de los usuarios. De hecho, multitud de voces señalan los peligros para la privacidad que tiene el especificar el lugar en que nos encontramos, ya que esa información de carácter personal permite rastrear nuestra posición en cada momento86). MANTELERO considera que "[l]as principales preocupaciones se derivan, concretamente, de la capacidad de estos sistemas para identificar y localizar a los usuarios a través de una monitorización que podría ser invasiva, especialmente cuando la información sobre la movilidad se asociara a datos provenientes de otras fuentes"87).

La vulneración de la intimidad de las personas por el uso de la geolocalización preocupa a nivel nacional tanto que la Agencia Española de Protección de Datos se está pronunciando cada vez con más frecuencia sobre este asunto88). A nivel europeo también se localizan esfuerzos en este sentido89). Destaca el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes90), que supuso un importante avance en la protección de datos del usuario ya que por primera vez se abordaba la geolocalización en los dispositivos móviles que tenían activada esta función por defecto91). El texto alerta como los proveedores de servicios de geolocalización pueden disponer de "una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un período de inactividad nocturna puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa". Y concreta que los proveedores deben eliminar los datos que recolecten una vez éstos no son pertinentes92). A raíz del Dictamen, para saber si los datos están protegidos normativamente ante aplicaciones inteligentes de movilidad que rastrean el movimiento hay que tener en cuenta los siguientes aspectos: estar informado de los fines a los que se van a destinar los datos de geolocalización que se van a tratar, dar el consentimiento previo, específico e informado, poder revocar el consentimiento en cualquier momento, y, conocer y ejercitar, cuando sea necesario, los derechos de acceso, rectificación, cancelación y oposición en relación con los datos recolectados.

Para determinar el marco legal de la geolocalización debemos de estar a lo establecido en el Reglamento General de Protección de Datos y la Directiva sobre la privacidad y las comunicaciones electrónicas93). El Reglamento entiende que los datos de localización son datos personales y, por tanto, merecedores de protección en los términos establecidos en la norma (art. 4). La Directiva define como dato de localización "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público (art. 2.c). Es más, la propia Directiva es consciente de la problemática que presenta los servicios de localización: "Tales datos constituyen datos sobre tráfico a los que es aplicable el artículo 6 de la presente Directiva. Sin embargo, además, las redes móviles digitales pueden tener la capacidad de tratar datos sobre localización más precisos de lo necesario para la transmisión de comunicaciones y que se utilizan para la prestación de servicios de valor añadido tales como los servicios que facilitan información sobre tráfico y orientaciones individualizadas a los conductores. El tratamiento de tales datos para la prestación de servicios de valor añadido sólo debe permitirse cuando los abonados hayan dado su consentimiento. Incluso en los casos en que los abonados hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización" (considerando 35).

La geolocalización debe respetar lo establecido en el Reglamento General de Protección de Datos que se aplica en todos los casos de tratamientos de datos personales como resultado del tratamiento de datos de localización. La Directiva, por su parte, solo se aplica al tratamiento de datos de las estaciones de base por servicios y redes públicas de comunicación electrónica (operadores de telecomunicaciones), de manera, que la norma afecta al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles a la ciudadanía en las redes públicas. Asimismo, establece la obligatoriedad del proveedor de un servicio de comunicaciones electrónicas a adoptar las medidas técnicas adecuadas para preservar la seguridad de sus servicios en colaboración con el proveedor de la red pública de comunicaciones (art. 4). Emplaza a los Estados miembros a garantizar, a través de su legislación nacional, la confidencialidad de las comunicaciones y de los datos de tráfico. Prohíbe expresamente "la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados", salvo ciertas excepciones (art. 5.1). Y señala que los datos de localización sobre usuarios de redes públicas de comunicaciones o servicios de comunicaciones solo se pueden tratar si se hacen anónimos o se obtiene el consentimiento del afectado, y solo para la medida y el tiempo necesario para añadir valor al servicio que se pretenda (art. 9.1).

A nivel interno, se debe estar, de manera general, a los principios establecidos en la Ley de Protección de Datos, que no aborda de manera expresa los servicios de localización94). Junto a esta, la Ley General de Telecomunicaciones señala el régimen aplicable al uso de datos de localización (según las directrices marcadas por la DDirectiva sobre protección y comunicaciones electrónicas). Así, se pueden usar los datos de localización de los usuarios de redes públicas de comunicaciones o servicios de comunicaciones electrónicas públicas cuando: los datos se hagan anónimos o cuenten con el consentimiento informado del usuario; solo podrán usarse en la medida y durante el tiempo necesario para prestar servicios de valor añadido; el usuario deberá conocer los datos a tratar, la finalidad y duración de los mismos y el servicio de valor añadido que se va a prestar; y, los usuarios deben tener la posibilidad de revocar el consentimiento dado para que traten sus datos de localización (art. 48.2. de la Ley General de Telecomunicaciones, que se complementa con el art. 9 de la Directiva sobre protección y comunicaciones electrónicas)95).

Así, a raíz de la normativa aplicable y las recomendaciones europeas podemos establecer que, para la utilización de los servicios de localización, cuyo protagonismo es indudable en la *smart mobility*, se requiere del consentimiento, informado y específico, del usuario para utilizar esos datos y ofrecer un servicio de valor añadido, del cual, deberá tener conocimiento exacto. El consentimiento no se puede dar como parte de las condiciones generales96). No obstante, los sujetos, ya sean públicos o privados, que utilicen datos sobre la ubicación del usuario, información de carácter personal, deben ser bastantes escrupulosos en cuanto a su tratamiento para evitar situaciones de dudosa legalidad. En ocasiones la localización del usuario se registra sin su consentimiento y sin tener la información necesaria, de hecho, recientemente han visto la luz escandalosos ejemplos en tal sentido97). Por todo ello, dado la indudable presencia de los servicios de geolocalización en las aplicaciones de movilidad inteligente se precisa de un adecuado marco legal que evite situaciones fraudulentas o ilícitas que supongan una merma de los derechos ciudadanos.

IV. CONCLUSIONES

1. La movilidad inteligente se ha erigido como elemento principal de la *smart city*, dada la importancia que los desplazamientos tienen en las ciudades. Sin embargo, pese a su creciente auge no existe un concepto único de lo que se entiende por movilidad inteligente.

La noción de *smart mobility* se encuentra íntimamente relacionada con el término de ciudad inteligente, del cual se disgrega. En gran parte la descripción de *smart mobility* dependerá de que lo que se entienda por ciudad inteligente, por lo que resulta complejo encontrar una definición única de movilidad inteligente. A nivel normativa destaca el escaso interés por ofrecer un concepto legal, tanto a nivel comunitario como interno.

En contraste, encontramos otro concepto relacionado con éste que goza de mayor parangón a nivel institucional y es el de movilidad sostenible. Ambas descripciones guardar grandes semejanzas y persiguen los mismos fines, de hecho, no se entiende una movilidad inteligente que no sea sostenible. Aunque es cierto que en el término *smart mobility* la referencia a las tecnologías es totalmente explícita.

Así, el concepto de *smart mobility* se halla en continuo proceso de formación, abierto a los cambios tecnológicos que se suceden y sin que exista consenso sobre éste. Aunque esto no es óbice para que su esencia y sus elementos definitorios estén meridianamente claros para la doctrina. La innovación constituye el eje vertebral del término, a partir de ahí, entran en juego aspectos comunes como la sostenibilidad, el respeto al entorno, la eficiencia de los recursos o la mejora de las infraestructuras.

2. Así, consideramos que la movilidad inteligente se configura como un sistema de movilidad caracterizado por el uso de las innovaciones tecnológicas para lograr una mayor eficiencia y eficacia. De ahí, podemos encontrar los dos patrones característicos de este fenómeno: la utilización de las tecnologías emergentes como columna vertebral del concepto y sistema eficaz y eficiente de cara a la consecución de los objetivos medioambientales y sociales. Mediante la aplicación de la inteligencia artificial a la red de transporte y los desplazamientos por la ciudad se consigue una movilidad respetuosa con el medioambiente y el entorno que redunda, a su vez, en una mayor calidad de vida en las ciudades. Así, la tecnología se usa de manera integrada y eficaz para alcanzar un transporte más limpio acorde con el desarrollo sostenible.

3. La relación que guarda la movilidad inteligente con las TIC presenta una cara del fenómeno escasamente tratada, como es su afección a la protección de datos personales. La incidencia de la movilidad inteligente en la protección datos personales de los usuarios es evidente. La *smart mobility* puede posibilitar la localización exacta del vehículo, que el coche reciba información en tiempo real sobre la situación de las vías, o lograr que las señales de tráfico sean dinámicas. Y es que mediante la adquisición de los datos del usuario y, su posterior tratamiento, se puede llegar a realizar un seguimiento de sus actividades y su movilidad geográfica, sus rutas habituales, sus preferencias de movilidad, incluso llegar a saber dónde trabaja y vive o sus lugares de ocio preferidos. Esto se consigue mediante el *big data* que permite la creación de perfiles del usuario a través de la minería de datos.

De manera que la información personal es el elemento principal de las aplicaciones que usan la inteligencia artificial. Esto nos aboca a un complejo panorama jurídico donde surgen numerosas cuestiones relacionadas con la problemática de la protección de los datos personales. La velocidad con la que se suceden los cambios en el entorno digital y el espacio transfronterizos donde se mueven los datos provocan que sea muy difícil una adecuada seguridad de los mismos. La falta de un adecuado marco normativo induce a situaciones que despiertan recelos e inseguridades a la hora de salvaguardar los derechos de los ciudadanos y agrava el despliegue de las estrategias inteligentes en nuestro país.

4. Los servicios de *smart mobility* pueden ser prestados, cuando no facilitados, por la propia Administración Pública. Como consecuencia, ésta recoge multitud de datos personales de los administrados que posibilita la identificación de patrones de movilidad de la ciudadanía, entre otras cuestiones. Una mala praxis en la gestión de los mismos podría conllevar a gobiernos que monitoricen a sus ciudadanos o conozcan los trayectos recurrentes de los mismos. Por ello, es necesario establecer mecanismos adecuados para velar por los derechos de los individuos frente a actuaciones que pueden soslayar la legalidad. Esto implica llegar a un nuevo paradigma donde las Administraciones Públicas ponderen los riesgos concurrentes en la protección de datos e innoven en formas que potencien su defensa, en aras del buen gobierno y en consonancia con la transparencia exigida al espacio público.

A todo ello, hay que unir que en la movilidad inteligente actúan diferentes actores con intereses contrapuestos. Además de la Administración Pública, dadas sus competencias en tráfico y movilidad; también concurren las empresas privadas, a las cuales puede recurrir la Administración para prestar servicios de interés general. En este sentido, el protagonismo de los actores privados es palpable habida cuenta de su papel en el desarrollo de aplicaciones de *smart mobility* o en su gestión en las redes de telecomunicaciones donde se transmite la información. Aunque la involucración de los agentes públicos o privados dependerá de cada proyecto de movilidad inteligente.

5. En relación con esa protección de datos, destaca a nivel normativo el Reglamento europeo que regula esta cuestión donde elementos como la trasferencia de datos a terceros o la explotación económica de los mismos coexisten con el reconocimiento al control de los datos que tiene la persona individual. Se presta atención a la defensa de la información de los usuarios y se repara en la importancia económica que tiene permitir el libre flujo de datos personales.

El primer aspecto destacable en cuanto a la nueva regulación es que se ha transitado desde una directiva hacia un reglamento con lo que ello implica jurídicamente. El resultado ha sido una norma compleja y amplia que dificulta la tarea de simplificar la materia, ardua de por sí. Esto puede producir la difícil comprensión por parte de los ciudadanos de los riesgos que entrañan las aplicaciones inteligentes y, por consiguiente, que el marco europeo se deje por el camino sus principales objetivos y la materia regulada acabe empañada por multitud de especificaciones técnicas.

No son pocos los autores que subrayan la insuficiente e inadecuada normativa sobre protección de datos acorde con el cambiante escenario donde éstos se mueven y, por ello, reclaman la definición de un marco jurídico y ético que regule el uso de información personal en la era del *big data* que aporte mayor seguridad jurídica al sistema y respete los derechos de los ciudadanos.

6. Frente a la recopilación de datos por las aplicaciones tecnológicas, algunos autores plantean el uso general de datos anónimos como medida de solución. En este sentido, el vigente Reglamento europeo de protección de datos opta por la seudonimización. Sin embargo, no está claro que transformar los datos de una persona en anónimos puedan impedir la identificación de esta, habida cuenta de la “inteligencia” de las tecnologías y sus algoritmos. En efecto, aunque los datos sean anónimos se obtiene tanta información de un sujeto concreto mediante el *big data* que a través de la trazabilidad de éstos se puede acabar descubriendo la persona a quien pertenece la información recogida. Además, con la seudonimización se mermaría la personalización de los servicios prestados por las aplicaciones, principal atractivo de las mismas, y se abriría la puerta a situaciones fraudulentas.

7. Otro aspecto especialmente importante en las aplicaciones de movilidad inteligente es la geolocalización. Así, las aplicaciones que utilicen esta función deben de informar al usuario de los fines a los que se va a destinar la información geolocalizada recogida, recabar el consentimiento previo del mismo y darle la posibilidad de revocar el mismo en cualquier momento. El Reglamento europeo de protección de datos considera que los datos de localización son datos personales y, por ello, quedan bajo su amparo. La Directiva sobre la privacidad y las comunicaciones electrónicas señala que los datos de localización solo pueden ser tratados si se convierten en anónimos o se obtiene el consentimiento del afectado y solo para la medida y el tiempo necesario para dar el valor añadido al servicio que se pretenda.

A pesar de esto, por la especial sensibilidad de esos datos se debe procurar un máximo celo a la hora de trabajar con ellos para evitar situaciones de precaria legalidad. No está de más recordar ejemplos de cómo, en ocasiones, la localización de los usuarios se ha registrado sin su consentimiento o los recelos que despierta entre la ciudadanía cuando esas actitudes provienen de un Gobierno. Así, es necesario un marco legal adecuado que evite situaciones tramposas habida cuenta del protagonismo de la geolocalización en las aplicaciones de *smart mobility*.

8. En cualquier caso, se hace preciso una adecuada regulación en torno a la materia para proteger los derechos constitucionales de los ciudadanos. La multitud de actores, especialmente de carácter privado, que intervienen en el contexto de la movilidad inteligente redunda en la necesidad de definir un marco legal que tome en consideración la nueva sociedad digital, habida cuenta de los diferentes y variopintos intereses que se concitan en la *smart mobility*. Es cierto, que el Reglamento europeo de protección de datos ha supuesto un paso importante, pero aún quedan cuestiones sin resolver, por no mencionar el cada vez más cuestionado consentimiento del titular de los datos, piedra angular de la norma. La avidez de las empresas tecnológicas que operan en este contexto para eludir los controles legales, la rapidez con la que se suceden los cambios en la sociedad digital y el espacio transfronterizos donde se mueven los datos hace que sea muy difícil salvaguardar los derechos ciudadanos. Por ello, se necesita un adecuado marco normativo que tenga en cuenta las variadas relaciones jurídicas subyacentes en el ámbito de la movilidad inteligente. En este sentido, hay autores que reclaman la urgente necesidad de definir un encuadre legal y ético que regule el despliegue de la tecnología inteligente no ya sólo en nuestro país, sino a nivel europeo e incluso mundial.

9. Así, el derecho fundamental a la protección de datos trata de aportar a la persona un control sobre sus datos personales, permitiéndole conocer su uso y destino. El consentimiento se configura como el eje central de la normativa sobre protección de datos. Sin ese consentimiento todo tratamiento de datos (con algunas salvedades) se considera ilícito. Sin embargo, en la actualidad, la realidad ha soliviantado los cimientos de tal concepción. La agudeza de las técnicas de recolección de datos en las diferentes aplicaciones informáticas, las cesiones de información entre las mismas, la creación de perfiles automáticos y las múltiples posibilidades que permite el *big data* provocan que el pilar fundamental del consentimiento quede en entredicho. Para una persona media resulta complejo conocer el alcance del tratamiento sobre el que se le pide el consentimiento o llegar a controlar de manera real y efectiva la información que está compartiendo.

Nuestro ordenamiento jurídico trata de asentar la idea de que toda persona puede mantener una vigilancia amplia sobre su información personal. Pero tal soflama resulta, en ocasiones, inviable. Es cierto que cada persona es libre de decidir qué hacer con sus datos. El valor que cada uno hace de su privacidad depende de diversos factores y del escenario en el que se actúe. De ahí que las normas sobre protección de datos permitan cierta flexibilidad en relación con las condiciones del tratamiento en función del contexto, siendo el usuario quien puede modular el régimen legal de acuerdo con su voluntad. No obstante, es preciso indicar que, en ocasiones, el consentimiento se convierte en un “engaño”. En vez de proporcionar al titular de los datos un control sobre los mismo, permite a las empresas una máxima operatividad sobre ellos. Por no mencionar que aquel que rechaza prestar su consentimiento en determinados servicios queda excluido de la sociedad digital imperante. Al igual que sería bastante inocente pensar que todo el consentimiento que se da se hace de forma libre. Y esto sin entrar en valorar el conocimiento del consentimiento ya que aun cuando el responsable ha informado previamente, se está presuponiendo que el usuario ha comprendido o leído completamente toda la información relativa a su privacidad. En realidad, el margen de decisión del usuario queda en entredicho. Y aunque el individuo puede ejercitar sus derechos de control a posteriori, pocas personas reparan en ello.

10. En efecto, la normativa sobre protección de datos trata de asentar el mantra de que el usuario de la sociedad digital posee un efectivo dominio sobre su información. La legislación expresa sus nobles propósitos, pero no llegan a gozar de efectividad real. Por ello, es necesario reforzar la transparencia de las aplicaciones que operan en la ciudad inteligente para que el derecho a la información de los interesados se haga valer. Éste tiene que conocer de manera clara, precisa y comprensible quién trata sus datos, cómo lo hace, con qué fin, durante cuando tiempo y los derechos de los que dispone.

La transparencia es la clave de la nueva sociedad digital. En el ámbito público, este elemento se relaciona con el acceso a la información por parte de la ciudadanía y mayor nitidez en la actividad administrativa. La transparencia conduce a la idea de control en relación con la noción de democracia y en aras del empoderamiento del ciudadano.

El principio de transparencia y el acceso a la información pública promueve la formación de una opinión pública sana, la participación en los asuntos públicos, el control democrático de las instituciones del Estado y redundan en un mayor funcionamiento de la Administración Pública. Sin embargo, esta concepción del principio de transparencia en sector público debería trasladarse al ámbito empresarial, ya que cada vez más, los individuos demandan información sobre las diferentes entidades que les prestan servicios que invaden su día a día y que están omnipresentes en su proceder cotidiano. La sociedad en su conjunto desea tener un mayor conocimiento de las decisiones relevantes que adoptan las empresas privadas para de este modo, dotar al usuario de un mayor conocimiento real y efectivo.

Es cierto, que el Reglamento General de Protección de Datos establece que los datos personales deben ser

tratados de forma lícita, leal y transparente en relación con el interesado; ensalzando el derecho a la transparencia, que queda incorporado en el mundo de la protección de datos. En este sentido, se ha intentado aportar luz en las normas en materia de consentimiento para garantizar que se proporcione de forma libre e informada. El responsable del tratamiento debe tomar las medidas oportunas para proporcionar al usuario toda la información relativa al trato de la misma. Pero en la compleja sociedad digital, el hecho de que un prestador de servicios tecnológicos cumpla con el deber de información no garantiza que el individuo pueda llegar a tener un conocimiento certero del tratamiento de sus datos. Creando, en definitiva, al usuario una imagen falsa de control o disposición sobre su información.

11. Junto al principio de transparencia, sería necesario repensar el modelo actual del consentimiento. Hay que proporcionar a los titulares de los datos un poder efectivo para decidir qué hacer con su información personal. Todo ello junto con un estricto cumplimiento de las obligaciones informativas. Las empresas que operan con datos personales de los usuarios deben redactar cláusulas de privacidad empleando términos más sencillos, concisos, pero también completos, sin margen para la ambigüedad o la abstracción. Se deben utilizar planteamientos claros para evitar confundir o aturdir al usuario98). En todo caso, hay que procurar que el consentimiento que se preste sea realmente informado y que el usuario pueda conocer el tratamiento real que se va a hacer de sus datos.

Y es que, frente a la voracidad informativa de la sociedad del conocimiento y el sentimiento generalizado de una pérdida de privacidad inevitable para operar con las aplicaciones relacionadas con la inteligencia artificial, se hace necesario superar los límites obsoletos en materia de protección de datos. Así, hay que trasladar el principio de transparencia del ámbito público al privado para generar un mayor cauce de información entre el prestador del servicio y el individuo, generando, así mayores cotas de confianza en la sociedad y en clara consonancia con la responsabilidad social corporativa que debe fomentar cada organización. Y, por otro lado, hay que repensar el modelo actual del consentimiento, convertirlo en un verdadero mecanismo de control del usuario. Ofreciendo una información nítida, con términos poco complejos o que inciten a la confusión, para que el titular de los datos sepa exactamente lo que está aceptando. Para construir una verdadera ciudad inteligente y promover la *smart mobility* es necesario que exista una mayor conciencia del sector privado, principal protagonista de este escenario, para generar confianza en la ciudadanía, que va a ser la principal receptora de las políticas *smart*.

V. BIBLIOGRAFÍA

AGEPD. *Protección de datos y Administración Local. Guías sectoriales AEPD*. Disponible en https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf.

ARROYO VÁZQUEZ, N. (2011). *Informe APEI sobre movilidad*. Disponible en http://www.apei.es/wp-content/uploads/2013/11/InformeAPEI-Movilidad.pdf.

ARIAS POU, M. (2016). “Definiciones a efectos del Reglamento General de Protección de Datos”, en PIÑAR MAÑAS, J.L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, pp. 115-133.

BBC. (2018). “Google rastrea tu localización incluso cuando le pides que no lo haga”. *BBC.com*. Disponible en https://www.bbc.com/mundo/noticias-45189915 .

BATUECAS CALETRÍO, A. (2015). “Intimidad personal, protección de datos personales y geolocalización”. *Derecho Privado y Constitución,* núm. 29, pp. 47-82. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5300038.

BARREDO, A. (2017). “Tus datos personales son tu propio pozo petrolífero”. *La Vanguardia*. Disponible en https://www.lavanguardia.com/tecnologia/20170121/413570434406/datos-personales-publicidad-google-facebook-amazon-foursquare.html.

CANTO LÓPEZ, M.T. (2017). “Administración Pública y participación activa del ciudadano en la gestión de la ciudad inteligente” en PIÑAR MAÑAS, J.L. *Smart Cities. Derecho y técnica para una ciudad más habitable*. Madrid: Reus, pp. 37-43.

CAO, G.; WANG, S.; HWANG, M.; PADMANABHAN, A.; ZHANG, Z. y SOLTANI, K. (2014). “A Scalable Framework for Spatiotemporal Analysis of Location-based Social Media Data”. *Computers, Environment and Urban Systems*, núm. 51, pp. 70–82. Disponible en https://arxiv.org/abs/1409.2826.

COLOMER HERNÁNDEZ, I. (2018). “A propósito de la compleja trasposición de la Directiva 2016/680 relativa al

tratamiento de datos personales para fines penales". *Diario La Ley*, núm. 9179. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6370894.

COTINO HUESO, L. (2017). "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata*, núm. 24, pp. 131-150. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6066829.

DAVARA RODRÍGUEZ, M.A. (2016). "Reglamento Europeo sobre protección de datos". *Actualidad administrativa*, núm. 7-8. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5598871.

DOCHERTY, I.; MARSDEN, G. y ANABLE, J. (2018). "The governance of smart mobility". *Transportation Research Part A: Policy and Practice*, vol. 115, pp. 114-125. Disponible en http://eprints.gla.ac.uk/148143/1/148143.pdf.

DURÁN CARDO, B. (2016). *La figura del responsable en el Derecho a la protección de datos.* Madrid: La Ley.

FERNÁNDEZ, M. (2016). *Descifrar las smart cities. ¿Qué queremos decir cuando hablamos de smart cities*? Barcelona: Megustaescribir (Penguin Random House).

FERNÁNDEZ CONTE, J. y LEÓN BURGOS, D. (2016). "Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea", en PIÑAR MAÑAS, J.L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, pp. 35-50.

FINNIS K, K. y WALTON, D. (2007). "Field observations of factors influencing walking speeds". *International Conference on Sustainability Engineering and Science*. Disponible en https://pdfs.semanticscholar.org/b58f/5f444637be79b8a09e66cee2babb989b2b25.pdf .

GARCÍA-MENÉNDEZ, M.; CERRUDO, C.; PALAO, M. y EL-YATTOUMI, K. (2015). "Smart Cities ante el desafío de la seguridad. La ciudad inteligente, escenario clave para el despliegue de las smart OT". *Smart OT Series*, núm. 2, pp. 1-33. Disponible en https://www.cci-es.org/documents/10694/232272/Serie+Smart+OT_02_Smart+Cities+ante+el+desaf%C3%ADo+de+la+se....pdf/18d30523-0ec3-43f5-9767-c6483723ecab.

GÓMEZ JIMÉNEZ, M.L. (2015). "Smart cities vs. Smart governance: ¿dos paradigmas de interrelación administrativa no resueltos aún?". *Revista de derecho urbanístico y medio ambiente*, núm. 300, pp. 53-85. Disponible en https://www.researchgate.net/publication/283730513.

GIFFINGER, R.; FERTNER, C.; KRAMAR, H. [et *al*.] (2007). *Smart Cities: Rankinf of European Medium-Sized Cities*. Centre Regional Science. Universidad Tecnológica de Viena. Disponible en http://smart-cities.eu/download/smart_cities_final_report.pdf.

KOMNINOS, N. (2011). "Intelligent cities: Variable geometries of spatial intelligence". *Intelligent Buildings International*, vol. 3, pp. 172-188. Disponible en https://www.researchgate.net/publication/233470549/download.

LATHIA, N.; SMITH, C.; FROEHLICH, J. y CAPRA, L. (2013). "Individuals among commuters: Building personalised transport information services from fare collection systems". *Pervasive and Mobile Computing*, núm. 9(5), pp. 643–664. Disponible en https://doi.org/10.1016/j.pmcj.2012.10.007.

LONG, Y. y SHEN, Z. (2015). *Geospatial Analysis to Support Urban Planning in Beijing* [en línea]. China: Springer International Publishing. Disponible en https://books.google.es/books?id=K4vDCgAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false.

LÓPEZ ÁLVAREZ, L.F. (2016). "La responsabilidad del responsable", en PIÑAR MAÑAS, J.L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, pp. 279-298.

MANVILLE, C. ; COCHRANE, G. ; CAVE, J. ; MILLARD, J. [*et al*.] (2014). *Mapping Smart Cities in the EU*. Disponible en http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET(2014)507480_E N.pdf.

MARTÍNEZ NIETO, A. (2014). "Aspectos jurídicos de la movilidad sostenible". *Diario La Ley*, núm. 8429. Disponible en http://laleydigital.laley.es.uma.debiblio.com/.

MELLADO RUIZ, L. (2015). “Transporte y movilidad sostenible”, en GONZÁLEZ RÍOS, I. (dir.) *Estudios jurídicos hispanos-lusos de los servicios en red (energía, telecomunicaciones y transportes) y su incidencia en los espacios naturales protegidos*. Madrid: Dykinson, pp. 497-522.

MARTÍN-FERNÁNDEZ, F.; CABALLERO-GIL, P. y CABALLERO-GIL, C. (2014). “Autenticación no interactiva para Internet de las Cosas” [en línea], en ÁLVAREZ, R.; CLIMENT, J.J. (eds.) [*et al*.]. *RECSI XIII, Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información*. Alicante: Publicaciones de la Universidad de Alicante, pp. 75-80. Disponible en http://rua.ua.es/dspace/handle/10045/40461.

MANTELERO, A. (2015). “Smart cities, movilidad inteligente y protección de los datos personales”. *Revista de Internet, derecho y política*, núm. 21, pp. 37-49. Disponible en https://idp.uoc.edu/articles/10.7238/idp.v0i21.2919/galley/2974/download/.

NARAYANAN, A. y FELTEN, E.W. (2014). *No silver bullet: De-identification still doesn't work*. Disponible en http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

NÚÑEZ GARCÍA, J.L. (2016). “El encargado del tratamiento”, en PIÑAR MAÑAS, J.L. (dir.). *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*. Madrid: Reus, pp. 326-340.

OECD. (2015). *Big Data and Transport: Understanding and assessing options*. International Transport Forum. Disponible en https://www.itf-oecd.org › docs › 15cpb_bigdata_.

OLIVER LALANA, A. D. y MUÑOZ SORO, J. F. (2014). “El mito del consentimiento, o por qué un sistema individualista de protección de datos (ya) no sirve para (casi) nada”, en VALERO TORRIJOS, J. *La protección de los datos personales en Internet ante la innovación tecnológica*. Navarra: Aranzadi, pp. 153-196.

ORELLANA, D. (2011). “Dime cómo te mueves y te diré quién eres: La movilidad como huella del comportamiento espacial de las personas”. Disponible en https://www.researchgate.net/profile/Daniel_Orellana2/publication/280733197_Dime_como_te_mueves_y_te_dire_quien_eres_La_movilidad_como_huella_del_comportamiento_espacial_de_las_personas/links/55c3cd9408aebc967df1b7e3/Dime-como-te-mueves-y-te-dire-quien-eres-La-movilidad-como-huella-del-comportamiento-espacial-de-las-personas.pdf .

OSBORNE CLARKE. (2016). *Smart Cities y contratación pública. La oportunidad del Plan Juncker Oportunidades en el ámbito de las entidades locales*. Disponible en http://www.foroinfraestructuras.com/eventos/Luis%20Castro.pdf .

PAPA, E. y LAUWERS, D. (2015). *Smart mobility: Opportunity or threat to innovate places and Cities*. 20th International Conference on Urban Planning and regional Development in the Information Society. Belgium: Competence Center of Urban and Regional Planning, pp. 542-550. Disponible en: http://westminsterresearch.wmin.ac.uk/16363/1/CORP2015_46-1.pdf.

PAYERAS CAPELLÀ, M.M.; PANIZA FULLANA, A.: MUT PUIGSERVER, M. e ISERN DEYÀ, A.P. (2014). “Privacidad en servicios turísticos basados en geolocalización”. *Revista de Derecho, Empresa y Sociedad*, núm. 5, pp. 78-93. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5241174 .

PÉREZ PRADA, F.; VELÁZQUEZ ROMERA, G.; FERNÁNDEZ AÑEZ, V. y DORAO SÁNCHEZ, J. (2015). “Movilidad inteligente”. *Economía industrial*, núm. 395, pp. 111-121. Disponible en http://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/395/FIAMMA%20PEREZ%20y%20OTROS.pdf.

PIÑAR MAÑAS, J.L. (2008). “Novedades en relación con la figura del encargado del tratamiento”, en ZABÍA DE LA MATA, J. (coord.). *Protección de datos: comentarios al Reglamento*. Valladolid: Lex Nova.

RAMS RAMOS, L. (2016). “Tratamiento y acceso del público a documentos oficiales”, en PIÑAR MAÑAS, J.L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, pp. 605-624.

ROBUSTÉ, F.; VERGARA, C.; THORSON, L. y ESTRADA, M. (2003). “Nuevas tecnologías en la gestión de autopistas. El peaje y los sistemas inteligentes de transporte”. *Economía industrial*, núm. 353, pp. 33-46. Disponible

en https://dialnet.unirioja.es/servlet/articulo?codigo=1006031.

RODRÍGUEZ BUSTAMANTE, P. (2015). “La movilidad inteligente en las ciudades”. *Momento digital.com*. Disponible en http://momento.digital/la-movilidad-inteligente-las-ciudades/ .

RUBINSTEIN, I. (2012). “Big Data: The End of Privacy or a New Beginning?”. *Public Law Research Paper*, núm. 12-56. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659.

SÁNCHEZ BARRILAO, J.F. (2015). *De la ley al reglamento delegado (Deslegalización, acto delegado y transformaciones del sistema de fuentes).* Pamplona: Thomson Reuters Aranzadi.

SCHUURMAN, D.; BACCARNE, B.; DE MAREZ, L. y MECHANT, P. (2012). “Smart Ideas for Smart Cities Investigating Crowdsourcing for Generating and Selecting Ideas for ICT Innovation in a City Context”. *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 7, núm. 3, pp. 49-62. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4357121&orden=408480&info=link.

SEGUÍ PONS, J.M. y MARTÍNEZ REYNÉS, M.R. (2004). “Revista Electrónica de Geografía y Ciencias Sociales”. *Scripta Nova*, vol. VI, núm. 170 (60). Disponible en http://www.ub.edu/geocrit/sn/sn-170-60.htm.

STARICCO, L. (2013). “Smart mobility opportunità e condizioni”. *TEMA, Jorunal of Land Use, Mobility and Environment*, vol.6, núm. 3, pp. 341-354. Disponible en: http://www.rmojs.unina.it/index.php/tema/article/view/1933/2111.

TANNER, A. (2017). “The Hidden Trade in Our Medical Data: Why We Should Worry”. *Scientific American*. Disponible en https://www.scientificamerican.com/article/the-hidden-trade-in-our-medical-data-why-we-should-worry .

VALERO TORRIJOS, J. (2012). *Derecho, Innovación y Administración Electrónica*. Sevilla: Global Law Press.

VALERO TORRIJOS, J. (2014). “Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria: implicaciones jurídicas desde la perspectiva de la innovación tecnológica” en VALERO TORRIJOS, J. y FERNÁNDEZ

SALMERÓN, M. *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información.* Navarra: Aranzadi Cizur menor, p. 631-667.

VALERO TORRIJOS, J. (2017). “El acceso y la reutilització de la información del sector público desde la perspectiva de la reforma de la administración electrónica”, en MARTÍN DELGADO, I. (dir.). *La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho*. Madrid: Instituto Nacional de Administración Pública, pp. 433-458.

VALLS PRIETO, J. (2018). “El uso de inteligencia artificial para prevenir las amenazas cibernéticas”, en VALLS PRIETO, J. (coord.). *Retos jurídicos por la sociedad digital.* Navarra: Thomson Reuters Aranzadi, pp. 77-106.

1 Actualmente, más de la mitad de la población mundial (55 por ciento) vive en núcleos urbanos y para 2050 esta cifra se espera que alcance el 68 por ciento. Vid., UNITED NATIONS. (2018). *World Urbanization Prospects: The 2018 Revision*. Disponible en https://esa.un.org/Unpd/Wup/Publications/Files/WUP2018-KeyFacts.pdf .

2 Según la Organización Mundial de la Salud, cada año mueren en el mundo 1,3 millones a causa de la contaminación atmosférica urbana. Vid., ORGANIZACIÓN MUNDIAL DE LA SALUD. Departamento de Salud Pública, Medio Ambiente y Determinantes Sociales de la Salud. *Los efectos sobre la salud.* Disponible en https://www.who.int/phe/health_topics/outdoorair/databases/health_impacts/es/index1.html .

3 ROBUSTÉ, F.; VERGARA, C.; THORSON, L. y ESTRADA, M. (2003). “Nuevas tecnologías en la gestión de autopistas. El peaje y los sistemas inteligentes de transporte”. *Economía industrial*, núm. 353, p. 33. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=1006031 .

4 La vigente Ley Orgánica 3/2018 de Protección de Datos, en su Exposición de Motivos, reconoce que “[…] las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso”.

5 Resumen de Conclusiones del Supervisor Europeo de Protección de Datos sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital [DOUE núm. 338, de 13 de diciembre de 2016].

6 Además, la actual configuración ministerial ideada por el presidente del Gobierno, Pedro Sánchez, incluye un Ministerio de

Transportes, Movilidad y Agenda Urbana, con la idea de lograr una movilidad sostenible, eficiente y segura. Una denominación novedosa que vino a dar continuidad al tradicional Ministerio de Fomento. Vid, Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales [BOE núm. 25, de 29 de enero de 2020].

7 Hay que tener en cuenta que en esta ocasión se ha apostado por un reglamento que tiene aplicabilidad directa en los Estados miembros (el anterior régimen en protección de datos se articulaba en una directiva) y no se necesita de ninguna norma de transposición en los Estados miembros. No obstante, España ha adaptado al ordenamiento el Reglamento europeo en la Ley Orgánica 3/2018, aunque ha ido más allá y ha incluido nuevos aspectos, algunos han auspiciado la controversia. Junto al Reglamento europeo hay que tener en cuenta la Directiva sobre el tratamiento de datos para fines penales, vid., Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo [DOUE núm. 119, de 4 de mayo de 2016]. La Directiva tenía que haber sido transpuesta a nuestro ordenamiento jurídico antes de principio de mayo de 2018, sin embargo, tal hecho no se ha producido a pesar de que el Ejecutivo lo contemplaba en Plan Anual Normativo de 2018. Al tratarse de derechos fundamentales la trasposición requiere de la aprobación de una ley orgánica, por lo que su tramitación parlamentaria es más ardua. En este sentido, vid., COLOMER HERNÁNDEZ, I. (2018). “A propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales”. *Diario La Ley*, núm. 9179. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6370894 .

8 La *smart city* se caracteriza por el uso de la tecnología en los aspectos cotidianos de una ciudad para lograr unos servicios eficientes y sostenibles. Aunque no existe un concepto único o legal del mismo. No obstante, esto no es obstáculo para que haya una aproximación global a los elementos definitorios del mismo. Según la doctrina, el uso de las TIC para mejorar la vida de los ciudadanos y posibilitar el desarrollo económico, social y medioambiental es el rasgo principal. A partir de ahí entran en juego aspectos como el respeto del entorno, la eficiencia o la sostenibilidad de los recursos e infraestructuras. En España, ninguna norma aporta un concepto legal de la *smart city*. Por el contrario, abunda numerosas descripciones por parte de la doctrina. Vid., KOMNINOS, N. (2011). “Intelligent cities: Variable geometries of spatial intelligence”. *Intelligent Buildings International*, vol. 3, p. 174. Disponible en https://www.researchgate.net/publication/233470549/download. MANVILLE, C.; COCHRANE, G.; CAVE, J. y MILLARD, J. [et *al*.] (2014). *Mapping Smart Cities in the EU*. Disponible en http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET(2014)507480_EN.pdf . SCHUURMAN, D.; BACCARNE, B.; DE MAREZ, L. y MECHANT, P. (2012). “Smart Ideas for Smart Cities Investigating Crowdsourcing for Generating and Selecting Ideas for ICT Innovation in a City Context”. *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 7, núm. 3, pp. 49-62. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4357121&orden=408480&info=link .

9 MANVILLE, C. ; COCHRANE, G. ; CAVE, J. ; MILLARD, J. [*et al.*], *op.cit*., p. 9.

10 Se refiere a las medidas que utilizan las ciudades para atraer inversiones y población que incremente su PIB. Con la incorporación de las TIC se crean nuevos servicios y productos que potencian diferentes e innovadores modelos de negocio.

11 Se refiere a la formación de los ciudadanos para lograr el empoderamiento de éstos en habilidades digitales o aspectos relacionados con la tecnología aplicada a las ciudades.

12 Se alude al uso de la tecnología en el sistema de transporte y logístico para que éste sea más eficiente y respetuoso con el medioambiente. Supone el fomento del transporte público, la apuesta por una movilidad limpia o la introducción de vehículos ecológicos, entre otros aspectos.

13 Contempla medidas para reducir la contaminación y mejorar la sostenibilidad que ayude a crear un entorno más verde, limpio y eficiente. En esta clasificación se incluiría el impulso de las redes eléctricas inteligentes, la introducción de los sistemas de medición inteligentes de consumo de energía y agua, o la edificación y planeamiento sostenible, entre otras.

14 Con tal término se alude a las medidas para lograr un gobierno y una administración abierta y accesible a la ciudadanía, ya sea desde la consecución de una administración electrónica, la agilización y modernización administrativa o la mayor participación de los ciudadanos en la gestión pública.

15 La *smart living* engloba servicios de seguridad como la videovigilancia inteligente, servicios sanitarios como la teleasistencia o la gestión más eficientes de las emergencias sanitarias.

16 En concreto, llama la atención que el reciente Plan de Innovación para el Transporte y las Infraestructuras no ofrece una definición de movilidad inteligente pese a la presencia omnipresente de tal noción a lo largo de todo el documento. Vid., GOBIERNO DE ESPAÑA. Ministerio de Fomento. (2018). *Plan de Innovación para el Transporte y las Infraestructuras (2018-2020)*. Disponible en https://www.fomento.gob.es/NR/rdonlyres/66DE13DA-C640-4FB7-B83A-E8E9C6A2FD70/149597/plan_de_innovacion_20182020.pdf .

17 Según el Parlamento Europeo, las acciones relacionadas con el medioambiente y la movilidad son los más comunes con el 33 por ciento y el 21 por ciento de las iniciativas inteligentes, respectivamente. Vid., MANVILLE, C. ; COCHRANE, G. ; CAVE, J. ; MILLARD, J. [et *al*.], *op. cit.,* p. 32.

18 GÓMEZ JIMÉNEZ, M.L. (2015). “Smart cities vs. Smart governance: ¿dos paradigmas de interrelación administrativa no resueltos aún?”. *Revista de derecho urbanístico y medio ambiente*, núm. 300, p.52. Disponible en https://www.researchgate.net/publication/283730513 .

19 PÉREZ PRADA, F.; VELÁZQUEZ ROMERA, G.; FERNÁNDEZ AÑEZ, V. y DORAO SÁNCHEZ, J. (2015). “Movilidad inteligente”. *Economía industrial*, núm. 395, p.121. Disponible en http://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/395/FIAMMA%20PEREZ%20y%20OTROS.pdf .

20 GIFFINGER, R.; FERTNER, C.; KRAMAR, H. [*et al.*] (2007). *Smart Cities: Rankinf of European Medium-Sized Cities*. Centre

Regional Science. Universidad Tecnológica de Viena. Disponible en http://smart-cities.eu/download/smart_cities_final_report.pdf .

21 DOCHERTY, I.; MARSDEN, G. y ANABLE, J. (2018). "The governance of smart mobility". *Transportation Research Part A: Policy and Practice*, vol. 115, pp. 118-121. Disponible en http://eprints.gla.ac.uk/148143/1/148143.pdf

22 STARICCO, L. (2013). "Smart mobility opportunità e condizioni". *TEMA, Jorunal of Land Use, Mobility and Environment*, vol.6, núm. 3, pp. 342-343. Disponible en http://www.rmojs.unina.it/index.php/tema/article/view/1933/2111 .

23 PAPA, E. y LAUWERS, D. (2015). *Smart mobility: Opportunity or threat to innovate places and Cities*. 20th International Conference on Urban Planning and regional Development in the Information Society. Belgium: Competence Center of Urban and Regional Planning, pp. 543-547. Disponible en http://westminsterresearch.wmin.ac.uk/16363/1/CORP2015_46-1.pdf.

24 Vid., COMISIÓN EUROPEA. (2001). *Social aspects of sustainable mobility*, Transport RTD Programme, p. 9. Disponible en http://transport-research.info/sites/default/files/thematic-analysis/20040809_155137_51313_social_aspects.pdf.

25 Vid., GOBIERNO DE ESPAÑA. Ministerio de Fomento. (2009). *Estrategia española de movilidad sostenible.* Disponible en https://www.fomento.es/recursos_mfom/pdf/149186F7-0EDB-4991-93DD-CFB76DD85CD1/46435/EstrategiaMovilidadSostenible.pdf. Aunque en los últimos tiempos se han aprobado normas autonómicas que inciden de manera expresa en el transporte y la movilidad. Véase, por ejemplo, Ley 12/2018, de 23 de noviembre, de transportes y movilidad sostenible de Asturias [BOE núm. 14, de 16 de enero de 2019]. La Junta de Andalucía tiene previsto aprobar la denominada Ley de ordenación del transporte y la movilidad sostenible. A finales de 2019, el Gobierno vasco dio luz verde al Proyecto de Ley de Movilidad Sostenible.

26 La Estrategia Española de Movilidad Sostenible fue aprobada por el Consejo de Ministros, de 30 de abril de 2009, como marco de referencia para las distintas políticas sectoriales de movilidad sostenible.

27 MARTÍNEZ NIETO, A. (2014). "Aspectos jurídicos de la movilidad sostenible". *Diario La Ley*, núm. 8429, p.3. Disponible en http://laleydigital.laley.es.uma.debiblio.com/ .

28 MELLADO RUIZ, L. (2015). "Transporte y movilidad sostenible", en GONZÁLEZ RÍOS, I. (dir.) *Estudios jurídicos hispanos-lusos de los servicios en red (energía, telecomunicaciones y transportes) y su incidencia en los espacios naturales protegidos*. Madrid: Dykinson, pp. 509-510.

29 En este sentido, la Ley de Economía Sostenible señala los principios básicos de la materia, pero no define de manera explícita el concepto de movilidad sostenible. Asimismo, tanto la mencionada Ley (Disposición adicional decimonovena) como la Ley de calidad del aire y protección de la atmósfera (Disposición adicional séptima) llaman a la elaboración de una ley estatal de movilidad sostenible.

30 Sobre el nuevo rol de la Administración Pública y de la omnipresencia de la tecnología digital en la vida social, vid., FERNÁNDEZ, M. (2016). *Descifrar las smart cities. ¿Qué queremos decir cuando hablamos de smart cities*? Barcelona: Megustaescribir (Penguin Random House).

31 LATHIA, N.; SMITH, C.; FROEHLICH, J. y CAPRA, L. (2013). "Individuals among commuters: Building personalised transport information services from fare collection systems". *Pervasive and Mobile Computing*, núm. 9(5), pp. 643–664. Disponible en https://doi.org/10.1016/j.pmcj.2012.10.007 .

32 GHD. (2014). "New traffic data sources". New Data Sources for Transport Workshop, BITRE. Disponible en https://www.bitre.gov.au/events/2014/files/GHD-report-new-technologies-workshop.pdf .

33 Gracias a la información que se puede obtener de estos sistemas, en Nueva Zelanda se seleccionaron zonas concretas de ciudades donde existían videocámaras para medir el flujo de peatones. A raíz de esta experimentación se pudo conocer el número de peatones, sus características y la velocidad de sus andares a partir de la primera imagen del peatón grabada hasta que sale de plano. Vid., FINNIS K, K. y WALTON, D. (2007). "Field observations of factors influencing walking speeds". *International Conference on Sustainability Engineering and Science*. Disponible en https://pdfs.semanticscholar.org/b58f/5f444637be79b8a09e66cee2babb989b2b25.pdf .

34 CAO, G.; WANG, S.; HWANG, M.; PADMANABHAN, A.; ZHANG, Z. y SOLTANI, K. (2014). "A Scalable Framework for Spatiotemporal Analysis of Location-based Social Media Data". *Computers, Environment and Urban Systems*, núm. 51, pp. 70–78. Disponible en https://arxiv.org/abs/1409.2826 .

35 Es tal la información que proporcionan estas tarjetas que en Beijing (China) se han extraídos los datos que suministran para comprobar el número de residentes con bajo poder adquisitivo que usa el transporte público e identificar trayectos según el nivel socioeconómico. Vid., LONG, Y. y SHEN, Z. (2015). *Geospatial Analysis to Support Urban Planning in Beijing* [en línea]. China: Springer International Publishing, pp. 169–192. Disponible en https://books.google.es/books?id=K4vDCgAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false .

36 SEGUÍ PONS, J.M. y MARTÍNEZ REYNÉS, M.R. (2004). "Revista Electrónica de Geografía y Ciencias Sociales". *Scripta Nova*, vol. VI, núm. 170 (60). Disponible en http://www.ub.edu/geocrit/sn/sn-170-60.htm .

37 RODRÍGUEZ BUSTAMANTE, P. (2015). "La movilidad inteligente en las ciudades". *Momento digital.com*. Disponible en http://momento.digital/la-movilidad-inteligente-las-ciudades/ .

38 OECD. (2015). *Big Data and Transport: Understanding and assessing options*. International Transport Forum. Disponible en https://www.itf-oecd.org › docs › 15cpb_bigdata_.

39 GARCÍA-MENÉNDEZ, M.; CERRUDO, C.; PALAO, M. y EL-YATTOUMI, K. (2015). "Smart Cities ante el desafío de la seguridad. La ciudad inteligente, escenario clave para el despliegue de las smart OT". *Smart OT Series*, núm. 2, p.23. Disponible en https://www.cci-es.org/documents/10694/232272/Serie+Smart+OT_02_Smart+Cities+ante+el+desaf%C3%ADo+de+la+se....pdf/18d30523-0ec3-43f5-9767-c6483723ecab .

40 Tal y como lo define el Reglamento General de Protección de Datos, en su artículo 4, es un tratamiento automatizado de

datos personales que se basa en usar estos datos personales para evaluar aspectos de la persona y analizar o predecir sus intereses, comportamiento y otras características.

41 BARREDO, A. (2017). “Tus datos personales son tu propio pozo petrolífero”. *La Vanguardia*. Disponible en https://www.lavanguardia.com/tecnologia/20170121/413570434406/datos-personales-publicidad-google-facebook-amazon-foursquare.html. Asimismo, Valls Prieto señala que “[l]a vigilancia en Internet no es algo nuevo. Sin embargo, como hemos señalado anteriormente, las nuevas técnicas de procesamiento y análisis de datos sí hacen que la revolución realizada en los servicios de inteligencia sea cuando menos fascinante. Y al mismo tiempo peligrosas. El espionaje masivo, tal y como se ha podido demostrar en el caso Snowden, permite tener controlada a cantidades ingentes de población y la reacción de la ciudadanía no se ha hecho esperar”. Vid., VALLS PRIETO, J. (2018). “El uso de inteligencia artificial para prevenir las amenazas cibernéticas”, en VALLS PRIETO, J. (coord.). *Retos jurídicos por la sociedad digital*. Navarra: Thomson Reuters Aranzadi, p. 82.

42 Estos autores reflexionan sobre los problemas de seguridad que plantea el Internet de las Cosas y propone soluciones técnicas, vid., MARTÍN-FERNÁNDEZ, F.; CABALLERO-GIL, P. y CABALLERO-GIL, C. (2014). “Autenticación no interactiva para Internet de las Cosas” [en línea], en ÁLVAREZ, R.; CLIMENT, J.J. (ed.) [*et al*.]. *RECSI XIII, Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información*. Alicante: Publicaciones de la Universidad de Alicante, p. 80. Disponible en http://rua.ua.es/dspace/handle/10045/40461 .

43 Sobre la actividad de la Administración en el escenario de la *smart city,* vid., CANTO LÓPEZ, M.T. (2017). “Administración Pública y participación activa del ciudadano en la gestión de la ciudad inteligente” en PIÑAR MAÑAS, J.L. *Smart Cities. Derecho y técnica para una ciudad más habitable*. Madrid: Reus, pp. 37-43.

44 VALERO TORRIJOS, J. (2017). “El acceso y la reutilitzación de la información del sector público desde la perspectiva de la reforma de la administración electrónica”, en MARTÍN DELGADO, I. (dir.). *La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho*. Madrid: Instituto Nacional de Administración Pública, p. 448.

45 *Ibíd*., p. 448.

46 RUBINSTEIN, I. (2012). “Big Data: The End of Privacy or a New Beginning?”. *Public Law Research Paper*, núm. 12-56. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659 .

47 Vid., OLIVER LALANA, A. D. y MUÑOZ, J. F. (2014). “El mito del consentimiento, o por qué un sistema individualista de protección de datos (ya) no sirve para (casi) nada”, en VALERO TORRIJOS, J. *La protección de los datos personales en Internet ante la innovación tecnológica*. Navarra: Aranzadi, pp. 153-196.

48 GOBIERNO DE ESPAÑA. (2017). *Datos abiertos y ciudades inteligentes: una visión alternativa desde el Derecho*. Disponible en https://datos.gob.es/sites/default/files/blog/file/pdf_informe_datos_abiertos_y_ciudades_inteligentes.pdf .

49 VALERO TORRIJOS, J. (2017), *op.cit.,* p.448.

50 CANTO LÓPEZ, M.T., *op.cit*., p. 43.

51 VALERO TORRIJOS, J. (2015), *op.cit.,* pp. 1031-1032.

52 GOBIERNO DE ESPAÑA. Ministerio de Industria, Energía y Turismo. (2016). *Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes.* Disponible en https://www.ontsi.red.es/ontsi/sites/ontsi/files/interoperabilidad_parte_4_soluciones_alternativas.pdf .

53 COTINO HUESO, L. (2017). “Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales”. *Dilemata*, núm. 24, p.136. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6066829.

54 Sobre la importancia de la “infraestructura humana” en el desarrollo urbanístico, vid., GIFFINGER, R., FERTNER, C., KRAMAR, H. [et al.], *op.cit*.

55 Algunos autores son más explícitos y consideran que los principales involucrados sería los ciudadanos, por un lado, y los bancos, órganos de contratación, promotores y constructores, compañías públicas/privadas, inversores, asesores (tecnológicos, financieros, legales y aseguradores), compañías de transportes y compañías de *big data.* Vid., OSBORNE CLARKE. (2016). *Smart Cities y contratación pública. La oportunidad del Plan Juncker Oportunidades en el ámbito de las entidades locales*, p.3. Disponible en http://www.foroinfraestructuras.com/eventos/Luis%20Castro.pdf .

56 La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [DOUE de 31 de julio de 2002], menciona expresamente como servicio con valor añadido la orientación vial o la información sobre el tráfico, entre otros.

57 AGEPD. *Protección de datos y Administración Local. Guías sectoriales AEPD*. Disponible en https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf .

58 La propia norma considera que este aspecto es un riesgo para el cual los responsables y encargados del tratamiento deberán determinar las medidas técnicas y organizativas apropiadas para evitar situaciones indeseables (art. 28. 2 LOPDGDD).

59 Para profundizar en la figura del encargado, vid., PIÑAR MAÑAS, J.L. (2008*)*. “Novedades en relación con la figura del encargado del tratamiento”, en ZABÍA DE LA MATA, J. (coord.). *Protección de datos: comentarios al Reglamento*. Valladolid: Lex Nova, p. 226.

60 NÚÑEZ GARCÍA, J.L. (2016). “El encargado del tratamiento”, en PIÑAR MAÑAS, J.L. (dir.). *Reglamento general de protección de datos. Hacia un modelo europeo de privacidad*. Madrid: Reus, p. 326. Aunque la posibilidad de formalizar en un contrato el encargo de un tratamiento a un tercero ya se recogía en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos (derogada por el actual RGPD).

61 LÓPEZ ÁLVAREZ, L.F. (2016). “La responsabilidad del responsable”, en PIÑAR MAÑAS, J.L. (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad.* Madrid: Reus, pp. 288-289.

62 RAMS RAMOS, L. (2016). “Tratamiento y acceso del público a documentos oficiales”, en PIÑAR MAÑAS, J.L. (dir.).

Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad. Madrid: Reus, p. 616.

63 Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000 (RTC 2000, 292). Ponente: Julio Diego González Campos. [BOE núm. 4, de 4 de enero de 2001].

64 Sobre estos obstáculos, vid., VALERO TORRIJOS, J. (2012). *Derecho, Innovación y Administración Electrónica*. Sevilla: Global Law Press, pp. 293-303.

65 CANTO LÓPEZ, M.T. (2017)., *op. cit.,* p.45.

66 VALERO TORRIJOS, J. (2014). "Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria: implicaciones jurídicas desde la perspectiva de la innovación tecnológica" en VALERO TORRIJOS, J. y FERNÁNDEZ SALMERÓN, M. *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información.* Navarra: Aranzadi Cizur menor, p. 63.

67 El Tribunal Constitucional se ha pronunciado sobre el alcance del derecho fundamental a la protección de datos personales en la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio de 1993 (RTC 1993, 254) (Ponente: Fernando García-Mon y González-Regueral) [BOE núm. 197, de 18 de agosto de 1993]; afirmando que el artículo 18.4 de la Constitución española consagra un derecho fundamental autónomo y diferente del derecho a la intimidad, ya que la mencionada disposición está añadiendo "una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas […]", mediante "un uso ilegítimo del tratamiento mecanizado de datos[…]". Asimismo, la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000 (RTC 2000, 292) (Ponente: Julio Diego González Campos) [BOE núm. 4, de 4 de enero de 2001]; delimita el concepto y el contenido del derecho a la protección de datos personales y lo diferencia del derecho a la intimidad. Mientras que el derecho a la intimidad protege de cualquier invasión a la vida personal y familiar de una persona, el derecho a la protección de datos trata de garantizar que la persona tenga "control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Por tanto, el objeto de ambos derechos es diferente. Por su parte, los datos de carácter personal son, según el Real Decreto 1720/2007, "los datos de carácter personal consisten en cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". Esto es, toda la información de una persona física como su nombre, apellidos, su documento nacional de identidad, su dirección de correo electrónico, su domicilio, su estado civil, su historial de páginas web visitadas, la dirección IP, imágenes o vídeos en los que aparezca, una conversación de teléfono, etc.

68 SÁNCHEZ BARRILAO, J.F. (2015). *De la ley al reglamento delegado (Deslegalización, acto delegado y transformaciones del sistema de fuentes).* Pamplona: Thomson Reuters Aranzadi.

69 Sobre los antecedentes normativos de protección de datos en Europa, vid., FERNÁNDEZ CONTE, J. y LEÓN BURGOS, D. (2016). "Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea", en PIÑAR MAÑAS, J.L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, pp. 35-50.

70 Vid., DAVARA RODRÍGUEZ, M.A. (2016). "Reglamento Europeo sobre protección de datos". *Actualidad administrativa*, núm. 7-8. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5598871. Además, en protección de datos, la página web de la Comisión Europea en su apartado sobre la materia detalla de manera didáctica el marco normativo europeo en protección de datos; y contiene el llamado paquete de protección de datos, el cual, agrupa el Documento de Trabajo de la Comisión que fue la base del Reglamento y otras disposiciones. Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es .

71 Sobre la figura del responsable del tratamiento de los datos, vid., DURÁN CARDO, B. (2016). *La figura del responsable en el Derecho a la protección de datos.* Madrid: La Ley.

72 Vid., VALLS PRIETO, J., *op. cit*., p. 92. "En este punto creo que, sin ser obligatorio por parte de la Directiva 2016/680, sería necesario y muestra de un buen tratamiento de los datos que la autoridad competente informase al solicitante de los datos de alguna de la información básica que se requiere en la Directiva 95/46 […]".

73 Considerando 13 de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte.

74 En la ya derogada Directiva 95/46/CE se utilizaba, por el contrario, el concepto de procesamiento de disociación para referirse a aquel por el que se modifica los datos personales para que no puedan atribuirse a una persona que pueda ser identificable o identificada.

75 Artículo 4 del Reglamento General de Protección de Datos.

76 ARIAS POU, M. (2016). "Definiciones a efectos del Reglamento General de Protección de Datos", en PIÑAR MAÑAS, J.L. (Dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus, p.128.

77 Vid., Dictamen 3/2015, de 28 de julio, del Supervisor Europeo de Protección de Datos que lleva por título *Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos*.

78 Considerando 30 del Reglamento 2016/679: "Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas".

79 ARIAS POU, M., *op. cit*., p.128.

80 Algunas empresas como Telefónica han puesto en marcha lo que han denominado "anonimización segura", materializada en el proyecto *Smart Steps,* el cual, utiliza datos anonimizados para realizar estudios y análisis que ofrecen a organizaciones empresariales, asegurando, según expresan, la privacidad y la seguridad y "respetando siempre las normas de las agencias de

Protección de Datos de cada país en el que trabajamos". Vid., la página web oficial sobre esta iniciativa: https://luca-d3.com/es/tecnologia-smart-steps/index.html .

81 STJUE de 16 de abril de 2015 (TJCE 2015, 161) (Sala Cuarta). Caso W.P. Willems y Otros contra Burgemeester van Nuth y Otros. Cuestión prejudicial núm. C 449/2012. Ponente: J. Malenovsky. Resolución que decidió sobre una cuestión prejudicial relativa a la interpretación de determinados artículos del Reglamento (CE) 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viajes expedidos por los Estados miembros en su versión modificada por el Reglamento (CE) 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009.

82 Los datos biométricos son una serie de parámetros físicos propios de cada persona que se utilizan para poder comprobar su identidad (como por ejemplo la huella dactilar o el iris del ojo). El Reglamento General de Protección de Datos, en su artículo 4, define los datos biométricos como aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópico".

83 Reglamento (CE) 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viajes expedidos por los Estados miembros en su versión modificada por elReglamento (CE) 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009[DOUE núm. 385, de 6 de abril de 2009].

84 Adam Tanner expuso en un libro como compañías privadas utilizaban datos personales (en este caso médicos) que eran anónimos en el mercado secundario de datos, posibilitando fácilmente la identificación de personas. El autor ha realizado varias investigaciones en este sentido para demostrar la facilidad de identificar a personas en particular pese a los actuales procesos existentes para anonimizar los datos. Vid., TANNER, A. (2017). "The Hidden Trade in Our Medical Data: Why We Should Worry". *Scientific American*. Disponible en https://www.scientificamerican.com/article/the-hidden-trade-in-our-medical-data-why-we-should-worry .

85 NARAYANAN, A. y FELTEN, E.W. (2014). *No silver bullet: De-identification still doesn't work*. Disponible en http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf .

86 ARROYO VÁZQUEZ, N. (2011). *Informe APEI sobre movilidad*. Disponible en http://www.apei.es/wp-content/uploads/2013/11/InformeAPEI-Movilidad.pdf .

87 MANTELERO, A. (2015). "Smart cities, movilidad inteligente y protección de los datos personales". *Revista de Internet, derecho y política*, núm. 21, p.39. Disponible en https://idp.uoc.edu/articles/10.7238/idp.v0i21.2919/galley/2974/download/ .

88 Como ejemplo se pueden citar la Resolución R/00520/2015 del procedimiento de Declaración de Infracción de Administraciones Públicas AP/00005/2015, instruido por la Agencia Española de Protección de Datos al Ayuntamiento de Las Palmas de Gran Canaria. Y la Resolución R/00956/2013 del procedimiento de Declaración de Infracción de Administraciones Públicas AP/00040/2012, instruido por la Agencia Española de Protección de Datos al Ayuntamiento de Dos Hermanas.

89 De hecho, hay un grupo de trabajo formado por representantes de las autoridades nacionales de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que se encarga de las cuestiones relacionadas con las directivas de protección de datos, entre ellos, la geolocalización.

90 COMISIÓN EUROPEA. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, de 16 de mayo de 2011, realizado por el Grupo de Trabajo del artículo 29. p.7.

91 Para profundizar en esta cuestión vid., ORELLANA, D. (2011). "Dime cómo te mueves y te diré quién eres: La movilidad como huella del comportamiento espacial de las personas". Disponible en https://www.researchgate.net/profile/Daniel_Orellana2/publication/280733197_Dime_como_te_mueves_y_te_dire_quien_eres_La_movilidad_como_huella_del_comportamiento_espacial_de_las_personas/links/55c3cd9408aebc967df1b7e3/Dime-como-te-mueves-y-te-dire-quien-eres-La-movilidad-como-huella-del-comportamiento-espacial-de-las-personas.pdf .

92 PAYERAS CAPELLÀ y otros autores explican el funcionamiento de los servicios de localización en los terminales móviles. "Por ejemplo, los dispositivos de Google y Apple utilizan diversas formas para comunicar la localización del usuario. Respecto a Google, el dispositivo solicita el permiso explícito del usuario cuando éste elige la opción de utilizar Wi-Fi como método de localización. El dispositivo de Google también almacena los datos de localización del usuario por un período limitado y estos datos son encriptados. Sin embargo, los dispositivos Apple tradicionalmente no han pedido explícitamente el permiso para guardar estos datos. Se descubrió que estos dispositivos almacenaban los datos de localización sin cifrar y durante un período largo de tiempo. Se generaba entonces un problema inmediato: los datos se almacenaban de una forma fácilmente legible en la máquina del usuario (es decir, los datos de localización se almacenaban en el ordenador del usuario cuando se sincronizaba con el dispositivo). Vid., PAYERAS CAPELLÀ, M.M., PANIZA FULLANA, A., MUT PUIGSERVER, M. y ISERN DEYÀ, A.P. (2014). "Privacidad en servicios turísticos basados en geolocalización". *Revista de Derecho, Empresa y Sociedad*, núm. 5, p. 81. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5241174 .

93 Aunque hay que tener en cuenta que la Directiva pronto será sustituida por el Reglamento sobre la privacidad y las comunicaciones electrónicas.

94 Aunque la vigente Ley se pronuncia sobre la geolocalización en el ámbito laboral (artículo 90). Para profundizar sobre el tema, vid., BATUECAS CALETRÍO, A. (2015). "Intimidad personal, protección de datos personales y geolocalización". *Derecho Privado y Constitución,* núm. 29, pp. 47-82. Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=5300038.

95 Vid., PAYERAS CAPELLÀ, M.M.; PANIZA FULLANA, A.; MUT PUIGSERVER, M. y ISERN DEYÀ, A.P., *op.cit.,* pp. 84-85.

96 En este sentido, resultan interesantes las recomendaciones realizadas por Grupo de Trabajo del artículo 29 de la Unión Europea. Vid., ERUOPEAN UNION. (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*. Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf .

97 BBC. (2018). "Google rastrea tu localización incluso cuando le pides que no lo haga". *BBC.com*. Disponible en

https://www.bbc.com/mundo/noticias-45189915 .

98 Por ejemplo, la Agencia Española de Protección de Datos propone presentar la información al usuario por casa. Una primera capa de información contendría un nivel básico de la información solicitada, presentada de forma estructurada. Y una segunda capa con esa información más detallada.