UNIVERSIDAD DE LEÓN

Facultad de Derecho

Trabajo de Fin de Máster

Derecho de la Ciberseguridad y el Entorno Digital

Enfoques políticos y normativos en el desarrollo y adopción de forma segura de los vehículos inteligentes. Perspectivas desde la ciberseguridad

Policy and regulatory approaches in the safely development and adoption of smart vehicles. Perspectives from cybersecurity

Autor: Lic. José Alberto Barrueto Rodríguez

Tutor: Dr. Luis Ángel Ballesteros Moffa

León, julio 2019

Dedicatoria

Este trabajo es un homenaje a mis padres, a mi esposa, suegros, familiares, amigos, colegas, compañeros de trabajo, maestros y profesores; que de una forma u otra han apoyado, aportado o de cualquier forma coadyuvado a mi crecimiento personal y profesional.

Agradecimientos

A Cuba mi patria, por facilitarme los medios que han contribuido a mi formación.

A la Fundación Carolina, a la Universidad de León y al Instituto Nacional de Ciberseguridad, todos de España, por brindarme la oportunidad de participar en esta primera edición del Máster Oficial en Derecho de la Ciberseguridad y el Entorno Digital.

A todos los profesores que han sido parte del claustro de este programa de formación posgraduada, por los conocimientos aportados, la colaboración y el apoyo inagotable; especialmente a los profesores coordinadores del máster: Dra. Isabel Durán Seco, Dr. Salvador Tarodo Soria y Dr. Francisco Pérez Bes, así como a mi tutor Dr. Luis Ángel Ballesteros Moffa.

A mis colegas y amigos de la primera edición del Máster Oficial en Derecho de la Ciberseguridad y el Entorno Digital; por la camaradería y familiaridad conformadas desde principio a fin, que ayudaron a sortear todos los retos y dificultades.

ÍNDICE

ABREVIATURAS Y ACRÓNIMOS

ADAS	Sistemas Avanzados de Ayuda a la Conducción
ASIET	Asociación Interamericana de Empresas de Telecomunicaciones
HMI	Interfaz Hombre-Máquina
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IMT	Telecomunicaciones Móviles Internacionales
INCIBE	Instituto Nacional de Ciberseguridad de España
IoT	Internet de las Cosas
ISO	Organización Internacional de Normalización
M2M	Máquina a Máquina
OTT	Servicios Superpuestos a Internet
RGPD	Reglamento General de Protección de Datos
SAE	Sociedad de Ingenieros Automotrices
ITS	Sistemas Inteligentes de Transporte
TIC	Tecnología de la Información y la Comunicación
UIT	Unión Internacional de Telecomunicaciones
UNECE	Comisión Económica de las Naciones Unidas para Europa

Resumen: En el presente trabajo de investigación se abordan la industria automovilística, su evolución reciente y las perspectivas de desarrollo a partir de la convergencia de las tecnologías del automóvil y las de la información y la comunicación. Se presentan, las diferentes acciones que se promueven e implementan en el plano nacional e internacional en estos últimos años, para favorecer la adopción de los vehículos inteligentes. Se caracteriza la actividad de los gobiernos en un entorno de transformación digital, especificando las peculiaridades que tiene en el caso de los vehículos inteligentes. A su vez, se identifican las formas o enfoques políticos y normativos que garantizan el desarrollo y adopción de forma segura de los vehículos inteligentes; identificando aquellas que mejor responden a una realidad dinámica y que faciliten de forma flexible e innovadora, atender a las constantes necesidades en términos de ciberseguridad, protección de los consumidores y mantenimiento de la confianza en la utilización de esta como tecnología emergente y de transformación digital.

Palabras Claves: Vehículos inteligentes, Automatización, Autonomía, Conectividad, Inteligencia Artificial, Internet de las Cosas, Políticas y Regulaciones.

Abstract: In the present research work the automotive industry is addressed, its recent evolution and the perspectives of development from the convergence of automotive technologies and those of information and communication. The different actions that are promoted and implemented at the national and international level in recent years to favor the adoption of smart vehicles are presented. The activity of governments is characterized in an environment of digital transformation, specifying the peculiarities that it has in the case of smart vehicles. At the same time, the political and normative forms or approaches that guarantee the safe development and adoption of smart vehicles are identified; identifying those that best respond to a dynamic reality and that facilitate in a flexible and innovative way, meet the constant needs in terms of cybersecurity, consumer protection and maintenance of confidence in the use of this as an emerging technology and digital transformation.

Key words: Smart Vehicles, Automation, Autonomy, Connectivity, Artificial Intelligence, Internet of Things, Policies and Regulations.

OBJETO Y OBJETIVOS DEL TRABAJO

El objeto de este estudio es:

Analizar el fenómeno de los vehículos inteligentes (conectados, semiautónomos y autónomos), las tendencias principales de su evolución; y la influencia que tienen las políticas públicas, las disposiciones normativas, la actividad regulatoria de los gobiernos y otras formas de intervención política y reglamentaria de los estados; sobre su desarrollo y adopción de forma segura, con énfasis en la perspectiva desde la ciberseguridad.

Este objeto se puntualiza mediante los objetivos específicos siguientes:

1) *Describir la industria automovilística, su evolución durante el siglo XXI y las perspectivas de desarrollo a partir de la convergencia de las tecnologías del automóvil y las de la información y la comunicación.*

2) *Examinar las diferentes acciones que se promueven e implementan en el plano nacional e internacional en estos últimos años, para favorecer la adopción de los vehículos inteligentes.*

3) *Caracterizar la actividad de los gobiernos en un entorno de transformación digital, especificando las peculiaridades que tiene en el caso de los vehículos inteligentes.*

4) *Identificar las formas o enfoques políticos y normativos que garantizan el desarrollo y adopción de forma segura de los vehículos inteligentes; y los retos a resolver para su mejora, con énfasis en la perspectiva desde la ciberseguridad.*

METODOLOGÍA

a) Planteamiento del problema y la hipótesis de la investigación

A partir de la información recopilada sobre el sector estudiado, para realizar un enmarcamiento teórico y práctico, teniendo en cuenta el objeto y los objetivos específicamente previamente determinados; como problema e hipótesis de la investigación, se establecen los siguientes:

Problema de la investigación: Cómo influyen o impactan las políticas públicas, las disposiciones normativas, la actividad regulatoria de los gobiernos y otras formas de intervención política y reglamentaria de los estados; en el desarrollo y adopción actual de forma segura y la evolución futura de los vehículos inteligentes, en especial en el ámbito de su ciberseguridad.

Hipótesis de la investigación: La gestión de los gobiernos debe adaptarse a las necesidades de la industria automovilística y los usuarios, para conseguir el desarrollo y adopción segura de los vehículos inteligentes; mediante formas flexibles, dinámicas y armonizadas de intervención política y reglamentaria de los estados, que faciliten su progreso de forma efectiva y cibersegura.

b) Fundamentación teórica y planificación de la investigación

Al ser el fenómeno de los vehículos inteligentes y su regulación un tema muy novedoso, para la elaboración del marco teórico y contextualizar su estudio, se realizó una revisión bibliográfica de la documentación publicada en diferentes soportes durante el siglo XXI. La localización de la documentación se realiza mediante el acceso a bibliotecas, bases de datos y medios digitales, principalmente de los gobiernos de las naciones que son la avanzada en esta actividad; así como de las organizaciones internacionales intergubernamentales y no gubernamentales, consultorías internacionales y agencias estatales que han abordado esta temática de estudio (Ej. 5GAA Automotive Association, ASIET, Deloitte, GSMA, PriceWaterhouseCoopers, UIT, UNECE).

c) Métodos de Investigación para el desarrollo del trabajo

Teórico-Jurídico: Este método permitió la conceptualización teórico-operacional de las relaciones jurídicas que se generan a partir de la utilización de los vehículos inteligentes, de los sujetos que intervienen en dicha relación; así como, posibilitó la materialización del diseño y la medición de los resultados obtenidos, a partir de las variables y categorías relacionadas con la temática de estudio.

Método Exegético-Analítico-Histórico: El apoyo en este método, radicó en determinar, el sentido y alcance de las políticas públicas, las disposiciones normativas, la actividad regulatoria de los gobiernos y otras formas de la intervención de los estados en esta actividad durante el periodo histórico analizado.

Método de Derecho Comparado: Las comparaciones permiten determinar similitudes y diferencias entre las normas técnicas y jurídicas en la materia, fundamentalmente de China, España, Estados Unidos de América, Latinoamérica y el Caribe, Rusia y la Unión Europea,; comparando luego con las reglas de cada nación o sistema, como pueden ser órganos estatales investidos de potestad para controlar o regular la actividad, buscando las semejanzas que poseen los distintos ordenamientos jurídicos, teniendo en cuenta los diferentes sistemas jurídicos contemporáneos.

Método Sociológico: Con el uso de las técnicas aportadas por este método, se ha realizado un estudio de la gestión de los gobiernos ante el fenómeno de los vehículos inteligentes, mediante técnicas como la observación y la revisión de documentos o fuentes de información sonora y audiovisual.

d) Resultados, conclusiones y recomendaciones

Al final de este trabajo se describen los resultados obtenidos, las conclusiones a las que se llega y las recomendaciones que se consideran proponer, vinculadas a la temática de estudio.

INTRODUCCIÓN

En el marco de la denominada "4ª Revolución industrial"; es fundamental que los gobiernos, las empresas y los individuos estemos preparados para la transformación digital y las tecnologías emergentes; en especial, la inteligencia artificial, la Internet de las Cosas, las comunicaciones de máquina a máquina y la quinta generación de tecnologías de comunicación móvil celular terrestre; todas relacionadas directa o indirectamente con la industria automovilística y los vehículos inteligentes.

Como hemos planteado, los vehículos inteligentes abarcan una gama de automóviles que forman parte de sistemas de transporte inteligentes; en los que para su automatización se conjugan las telecomunicaciones (vehículos conectados) y diferentes tecnologías de la información y las comunicaciones en el ámbito del transporte por carretera; que pueden conformarse en apoyo de la labor de conducción (ADAS) o como verdaderos sistemas operativos avanzados, con capacidad de autoconducción (semiautónoma o totalmente autónoma), así como para las interfaces con otros modos de transporte.

Este específico proceso de digitalización de la sociedad, propicia, de forma incremental, cambios cada vez más rápidos y profundos en las sociedades y economías, constituyendo al mismo tiempo una fuerza disruptiva en muchos sectores; de lo cual no puede escapar la actividad de toma de decisiones políticas y reglamentarias a escala nacional, regional o mundial; exigiendo de los gobiernos una rápida adaptación a la evolución tecnológica, que sin embargo, en muchos países resulta sumamente difícil.

Debido a esa situación, se ha considerado importante, abordar en el presente trabajo de investigación, los enfoques que en materia de política y reglamentación constituyan las mejores prácticas específicamente en la materia de los vehículos inteligentes; de forma que se puedan identificar aquellas, que mejor responden a una realidad dinámica y que faciliten de forma flexible e innovadora, atender a las constantes necesidades en términos de ciberseguridad, protección de los consumidores y mantenimiento de la confianza en su utilización, como tecnología emergente y de transformación digital.

CAPÍTULO I - LOS VEHÍCULOS INTELIGENTES COMO EXPRESIÓN DE LA CONVERGENCIA DE LAS TECNOLOGÍAS DEL AUTOMÓVIL Y LAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

I.1 La industria automovilística de la nueva era

Desde que a finales del siglo XIX y principios del XX comenzó el avance del sector automovilístico, este ha sido líder en la investigación e innovación, cuando se le comparaba con otras actividades industriales; aunque actualmente, su devenir está sujeto al actuar de otros actores que no han sido los tradicionales, pero que en el siglo XXI se han convertido en sus impulsores[1].

La producción de automóviles a escala global superará el umbral de los 100 millones en 2019. Aunque hoy en día se producen 3.000 modelos diferentes en más de 700 fábricas, sólo el 2% son vehículos totalmente eléctricos. Estos no serán los únicos que circularán en el futuro, coexistiendo diferentes modelos de propulsión en un horizonte a corto/medio plazo. Los datos representarán el combustible del futuro modelo de negocio de esta industria, obteniendo ingresos por su utilización. Al mismo tiempo, el empuje del coche compartido y la llegada de los vehículos inteligentes (semiautónomos, totalmente autónomos o sin conductor) ocasionarán una drástica caída de los ingresos en el sector[2].

Informes recientes han concluido que empresas incluyendo los fabricantes de automóviles dominantes en el mercado, gigantes tecnológicos y startups especializadas, han invertido $ 50 mil millones de USD en los últimos 5 años para desarrollar tecnologías de los

[1]Actualmente la iniciativa en el automóvil, la tienen compañías eléctricas, entidades financieras y principalmente fabricantes de terminales de comunicación, operadores de servicios OTT, de servicios de la sociedad de la información y gigantes de internet como Google, Apple, Tesla, y hasta la empresa propietaria del buscador chino Baidu, que planea poner autobuses autónomos en carretera en un plazo de dos o tres años en dicho país.

[2] CC.OO., Á.D.E.E.S., 2018. Situación y perspectivas en el sector del automóvil. Medidas ambientales, digitalización y automatización de la industria. [en línea]. Madrid, España: CC.OO Área de Estrategias Sectoriales. [Consulta: 23 enero 2019]. Disponible en: http://www.industria.ccoo.es/30f03016ef175ac370e57b5f43e44267000060.pdf.

vehículos autónomos, proviniendo el 70% de este monto de agentes externos al sector del automóvil[3].

El impacto del transporte compartido y del desarrollo tecnológico habrá cambiado el mercado de automoción drásticamente para 2030. En Europa se espera que el parque de vehículos se reduzca un 25%, de 280 millones a 200 millones de unidades y en Estados Unidos un 22%, de 270 a 212 millones de coches en 2030[4].

Los vehículos autónomos como parte de los sistemas inteligentes de transporte (STI) están transformando la eficiencia, la comodidad, la seguridad y el impacto medioambiental del transporte por carretera; su influencia también será palpable cada vez más para las personas con necesidades especiales y en la evolución de otras formas de transporte. Las estadísticas presentadas en diferentes estudios internacionales han permitido apreciar las tendencias principales de desarrollo de esta industria en los próximos años[5].

I.1.1 Vehículos eléctricos, pero de fuentes renovables

El 95% de los coches nuevos que se matriculen en 2030 serán eléctricos (55%) o híbridos (40%); sin embargo esta transición hacia un mercado de movilidad libre de emisiones será imposible sin la electrificación del parque móvil que, además, se alimentaría de fuentes renovables de energía.

En la actualidad en toda España hay unos 3.500 puntos de recarga para coches eléctricos, pero a finales de 2019, deberían ser más del triple de esta cifra; varios cientos de ellos se instalarán en carreteras, sobre todo en gasolineras situadas en las principales vías españolas, varias son las operadoras que harán posible cruzar el país con un coche eléctrico: Endesa, Iberdrola, Cepsa y Nissan, son las que más están empujando en este

[3]KPMG INTERNATIONAL, 2019. *2019 Autonomous Vehicles Readiness Index.* [en línea]. Ginebra, Suiza: KPMG International. [Consulta: 25 marzo 2019]. 136024-G. Disponible en: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf.
[4] KOSTER, ALEX; KUHNERT, FELIX; STÜRMER, C., 2017. Five trends transforming the Automotive Industry. [en línea]. S.l.: PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. [Consulta: 25 marzo 2019]. Disponible en: https://www.pwc.at/de/publikationen/branchen-und-wirtschaftsstudien/eascy-five-trends-transforming-the-automotive-industry_2018.pdf.
[5]Ídem.

sentido[6]. También habrá muchos más puntos donde cargar el coche en las vías públicas urbanas.

En el caso español, estas acciones se enmarcan o contribuyen, a la implementación de la Estrategia Española de Desarrollo Sostenible, aprobada en el 2007, basada en la Estrategia Europea con igual fin y la Estrategia de Impulso del vehículo con energías alternativas (VEA) en España (2014-2020); igualmente forman parte del contenido del Proyecto de Ley de medidas urgentes para la transición energética y la protección de los consumidores (procedente del Real Decreto-ley 15/2018, de 5 de octubre), tal como fue publicado en el Boletín Oficial de las Cortes Generales Núm. A-31-1, de fecha 26 de octubre de 2018, por el Congreso de los Diputados[7].

I.1.2 El coche autónomo lento pero seguro

De las cinco grandes tendencias, la del vehículo plenamente autónomo[8] se estima que será la que más tardará en hacerse realidad en la vida cotidiana de las personas. Se prevé que hacia 2022-2023 salgan al mercado los primeros vehículos con un nivel 4 de automatización[9], el nivel 5 marca la conducción totalmente autónoma[10] y que en 2030

[6] CANO, V., 2019. Las 6 tendencias en el automóvil que marcarán 2019. [en línea]. [Consulta: 25 marzo 2019]. Disponible en: https://www.autobild.es/listas/6-tendencias-automovil-que-marcaran-2019-349119.

[7] En este proyecto legislativo se establece como uno de sus fundamentos que las alternativas a los combustibles fósiles, especialmente los vehículos eléctricos, requieren un impulso normativo que resuelva los problemas de coordinación que impiden su implantación masiva. Entre las barreras principales se encuentra el insuficiente desarrollo de las infraestructuras de recarga, que detrae a muchos usuarios de adquirir un vehículo eléctrico enchufable ante la baja disponibilidad de puntos de recarga públicos.

[8] En la Instrucción No. 15/V-113 de la Dirección General de Tráfico del Ministerio del Interior, de 13 de noviembre de 2015, sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general; se define como vehículo autónomo a todo vehículo con capacidad motriz equipado con tecnología que permita su manejo o conducción sin precisar la forma activa de control o supervisión de un conductor, tanto si dicha tecnología autónoma estuviera activada o desactivada, de forma permanente o temporal. A estos efectos, no tendrá consideración de tecnología autónoma aquellos sistemas de seguridad activa o de ayuda a la conducción incluida como equipamiento de los vehículos que para su manejo o conducción sí requieran necesariamente control o supervisión humana activa. Son objeto de esta instrucción aquellos vehículos que incorporan tecnología con funciones asociadas a los niveles automatización 3,4 y 5 recogidos en Anexo No. 1 del presente trabajo.

[9] Ver Anexo No. 1 del presente trabajo.

[10] La Sociedad de Ingenieros Automotrices (SAE por sus siglas en inglés), una organización enfocada al desarrollo de los estándares tecnológicos para todo tipo de vehículos; promulgó en enero de 2014 el estándar SAE J3016 “Taxonomía y definiciones de los términos relacionados con los sistemas de automatización de la conducción para vehículos de motor en carretera”, su versión más actualizada es de junio de 2018; que presenta una serie de niveles que permiten cuantificar el progreso en la automatización de los automóviles, aunque no impone requisitos a sus fabricantes sino que es algo meramente informativo y orientativo. La SAE, creó una escala de seis niveles que permite medir la autonomía de los vehículos. Esta escala va desde el 0 hasta el cinco, donde el cero sería una automatización inexistente, y el 5 sería el de un vehículo totalmente autónomo. Estos distintos estadios de desarrollo son bien conocidos en la industria

todavía entre el 85% y el 90% de los coches sean conducidos por personas. No obstante, la velocidad del cambio dependerá no solo del desarrollo tecnológico, sino también de la capacidad de dotarse de regulaciones que faciliten o coadyuven a esta situación.

En China, desde marzo de 2018, la empresa Baidu empezó a probar sus coches autónomos en su capital de Beijing; este gigante tecnológico chino, recibió las primeras licencias para probar coches autónomos en 33 vías con 105 kilómetros de recorrido en total, en los suburbios menos poblados de la ciudad, siendo la primera compañía en recibir licencias para realizar pruebas de carretera abiertas en la ciudad. Baidu está avanzando, a medida que esta nación asiática trata de posicionarse como líder en este sector[11]; en noviembre de 2018 esta propia empresa firmó con la automovilística sueca Volvo, un acuerdo[12] para desarrollar conjuntamente vehículos eléctricos y totalmente autónomos, con el objetivo de producirlos en masa en este país, para que sea el mercado de vehículos autónomos más grande del mundo en las próximas décadas.

En España el límite genérico vías convencionales, se reduce en 10 km/h. Desde el 28 de enero de 2019, en carretera solo se podrá circular a 90 km/h[13]. Esta medida afectará a unos 10.000 km de la Red de Carreteras del Estado. Hacia mediados de año, también se aplicará en todas las ciudades una nueva velocidad máxima: 30 km/h. El riesgo de morir en un atropello se reduce entre 5 y 8 veces, cuando la velocidad se reduce de 50 a 30 km/h[14].

La lista de los sistemas de seguridad que deberán llevar todos los coches a la venta en la Unión Europea desde 2021, se cerrará este año y como sucede con muchas de estas

automovilística, entre los proveedores de servicios de telecomunicaciones o las empresas que investigan en soluciones de inteligencias y visión artificial. El estándar SAE J3016 fue adoptado por el Departamento de Transporte de EUA en septiembre de 2016; por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en 2015; y por la Unión Europea a la que se ha referido en su estrategia de despliegue de vehículos autónomos.

[11] FRANCIS CHAN, T., 2018. Baidu empieza a probar sus coches autónomos en Pekín. [en línea]. [Consulta: 25 marzo 2019]. Disponible en: https://www.businessinsider.es/baidu-empieza-probar-sus-coches-autonomos-pekin-197058.

[12] Baidu contribuirá con su plataforma de conducción autónoma Apollo, mientras que Volvo proporcionará acceso a su experiencia y tecnologías avanzadas de la industria de la automoción.

[13] El Consejo de Ministros de España aprobó el 28 de diciembre de 2018 la modificación del artículo 48 del Reglamento General de Circulación referido a los límites de velocidad en las carreteras convencionales con el fin principal de reducir la siniestralidad vial y cumplir el objetivo establecido en la estrategia de Seguridad Vial 2011-2020 de bajar de 37 la tasa de fallecidos en accidente de tráfico por millón de habitantes. En 2017 la tasa fue de 39.

[14]CANO, V., 2019. Las 6 tendencias en el automóvil que marcarán 2019. [en línea]. [Consulta: 25 marzo 2019]. Disponible en: https://www.autobild.es/listas/6-tendencias-automovil-que-marcaran-2019-349119.

obligaciones, numerosas marcas las aplicarán antes de la fecha inicial. Entre las 11 medidas que se barajan están: un sistema de registros de datos de eventos, una señal de detención de emergencia, mejora en la protección frontal con nuevos cinturones de seguridad y pruebas más exigentes en las pruebas de colisiones[15].

Los otros sistemas entre los que se incluyen sistemas avanzados de ayuda a la conducción (ADAS) en vehículos, que deberán llevar todos los coches europeos son: protección adicional para la cabeza de los peatones en caso de atropello, cristales de seguridad, control adaptativo de velocidad con radar frontal, asistente de mantenimiento de carril activo, refuerzos en la estructura lateral para mejorar en el test de colisiones y cámara trasera o un sistema de detección. La lista podría incluso ampliarse a 15 medidas[16].

Dos hitos relacionados con este tema a nivel español lo marcan:

- Lanzamiento el 9 de febrero de 2017 de la visión o patrón NERTRA[17] (Nueva Era del Transporte) acuñada por el capítulo español de la Asociación Internacional de Sistemas de Vehículos No Tripulados (AUSI-SPAIN) durante el congreso Diálogo 2017, celebrado en León.

- El anuncio en fecha 11 de abril de 2019 de la futura implementación a partir de la segunda mitad del 2019 en el campus de Vegazana de la Universidad de la León, del primer proyecto piloto a realizarse en este país por vías transitadas y que tiene como fecha de culminación hasta el 2022 para toda la ciudad. Este proyecto está

[15] Según la Dirección General de Tráfico en su Informe y análisis de octubre de 2016 sobre influencia de los sistemas de ayuda a la conducción en la seguridad vial y su aplicación para la clasificación de vehículos, los Sistemas de Asistencia a la Conducción (ADAS por sus siglas en inglés), permitirían la reducción del riesgo de siniestro en un 57% de los accidentes registrados en España. Un total de 51.000 accidentes que se evitarían o sus consecuencias se verían mitigadas significativamente.

[16]CANO, V., 2019. Las 6 tendencias en el automóvil que marcarán 2019. [en línea]. [Consulta: 25 marzo 2019]. Disponible en: https://www.autobild.es/listas/6-tendencias-automovil-que-marcaran-2019-349119

[17] A partir de lo que refiere AUSI SPAIN en su web oficial, NERTRA es un patrón definido por los vehículos autónomos que están alumbrando un nuevo horizonte, la automatización del transporte, siendo exigente en su orden de despliegue y supone un cambio de paradigma en la forma en la que se concibe el desplazamiento o la movilidad. Su impacto social, favorecerá el éxito social y personal. Su impacto económico, tecnológico e industrial, impulsará el nacimiento de nuevos sectores industriales y añadirá valor al tejido empresarial implicado. Su impacto sobre el PIB es tan relevante que cabe escindir entre los que se sumen a la NERTRA y los que no. Este patrón de movilidad es concordante con la legislación medioambiental en vigor y con las nuevas oleadas de legislación medioambiental que se avecinan, al hilo de los acuerdos formalizados en la Cumbre sobre el clima y la proliferación de alertas medioambientales extremas, por contaminación, en todo el mundo.

relacionado con vehículos autónomos nivel 4 y 5, enmarcándose dentro del proyecto pionero en Europa, impulsado por el capítulo español de la Asociación Internacional de Sistemas de Vehículos No Tripulados (AUSI-SPAIN) y con la implicación directa de la compañía de ingeniería y diseño de movilidad "DROTIUM".

I.1.3 Uno de cada tres kilómetros en coche serán 'compartidos'

Los propios automóviles comienzan a estar conectados en red, por lo que operan en condiciones más seguras, creándose nuevas propuestas de valor para, en última instancia, no generarse la necesidad de tener un vehículo propio; se van implantando elementos a través de conexiones móviles que permiten propuestas de valor agregado de transporte completamente diferentes, que tendrán repercusiones colaterales y profundas para los fabricantes y vendedores de automóviles, así como para las infraestructuras inalámbricas y de transporte correspondientes[18].

En los próximos años, se irá extendiendo una apuesta por el uso y disfrute de manera compartida del vehículo en lugar de su propiedad. Una vez se despejen las dificultades técnicas y las incertidumbres desde el punto de vista regulatorio, los kilómetros de transporte compartido crecerán sustancialmente. En la actualidad, menos de 1% de los trayectos en coche en Europa se corresponden con servicios de transporte compartido. Un porcentaje que en 2030 podría alcanzar el 35% de los kilómetros en el Viejo Continente, el 34% en Estados Unidos y el 46% en China[19].

General Motors (GM) está introduciendo cambios en su programa de vehículos compartidos Maven para que todos los vehículos de GM puedan utilizarlo. De esta forma, los propietarios de cualquier automóvil GM podrán compartirlo con otros usuarios. Además, un número creciente de fabricantes, como Porsche, Audi, Volvo, Lexus o Ford,

[18] ZHAO, HOULIN; LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN; FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.

[19]KOSTER, ALEX; KUHNERT, FELIX; STÜRMER, C., 2017. Five trends transforming the Automotive Industry. [en línea]. S.l.: PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. [Consulta: 25 marzo 2019]. Disponible en: https://www.pwc.at/de/publikationen/branchen-und-wirtschaftsstudien/eascy-five-trends-transforming-the-automotive-industry_2018.pdf.

están introduciendo programas de conexión inalámbrica para abonados, que permiten a sus miembros intercambiar vehículos de forma gratuita por semanas, meses, o según les sea más conveniente[20].

I.1.4 El coche automatizado conectado será toda una realidad en 2030

Una conectividad que se desarrollará en tres ámbitos: entre los vehículos, con las redes e infraestructuras de transporte y entre los ocupantes de los coches y el mundo exterior, lo que les permitirá trabajar, navegar por Internet y tener acceso a todo tipo de servicios multimedia durante los trayectos. En Europa[21] y en Estados Unidos en torno al 70% de los coches estarán conectados en 2030 y en China será el 100% los que disfrutarán de una conectividad total[22].

De acuerdo con los datos de Machina Research[23], el número de vehículos conectados listos de fábrica en todo el mundo llegará a 366 millones para 2025. En Europa, la regulación eCall[24] significó que todos los nuevos modelos debían tener módulos de telecomunicación móvil con tecnología 2G o 3G integrados a partir de marzo de 2018, para advertir automáticamente a los servicios de emergencia en caso de un accidente.

---

[20]ZHAO, HOULIN; LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN; FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.

[21] Según la Resolución del Parlamento Europeo, de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos (2018/2089(INI)), se espera que el nuevo mercado de vehículos automatizados y conectados crezca exponencialmente, con unos ingresos estimados en más de 620 000 millones EUR en 2025 para la industria automovilística de la Unión Europea y más de 180 000 millones EUR para su sector de electrónica.

[22]KOSTER, ALEX; KUHNERT, FELIX; STÜRMER, C., 2017. Five trends transforming the Automotive Industry. [en línea]. S.l.: PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. [Consulta: 25 marzo 2019]. Disponible en: https://www.pwc.at/de/publikationen/branchen-und-wirtschaftsstudien/eascy-five-trends-transforming-the-automotive-industry_2018.pdf.

[23] GSMA, 2018. Manual de Políticas Públicas de Telecomunicaciones Móviles 2019. Una guía de temas clave. [en línea]. S.l.: GSMA. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

[24]El sistema de llamada automática eCall instalado en los automóviles, permite que, en caso de accidente grave, se envíe automáticamente un mensaje al teléfono de emergencias a través de los centros 112; garantiza un acceso eficaz, directo y sin intermediación, a los centros competentes en gestión de demanda de emergencias, indicando los datos básicos del accidente para procurar una movilización efectiva de los servicios de emergencia. El servicio eCall, facilita la rápida aplicación de los protocolos establecidos en función de la localización y tipología, de forma que aquellos servicios a movilizar–ambulancias, rescate, policiales, etc.– están inmediatamente informados de todos los datos de que se dispone. Con eCall, además, se obtiene información adicional y precisa sobre la localización exacta del accidente, la identificación del vehículo, su tipología, etc.

Según el informe sobre el Índice de Preparación para Vehículos Autónomos 2019 (AVRI, por sus siglas en inglés), publicado por KPMG International[25], segundo estudio de esta consultora que evalúa la preparación en términos de avance y capacidad de 25 países[26], en la introducción de los vehículos autónomos debe tenerse en cuenta cuatro pilares integrales: *Política y legislación, Tecnología e innovación, Infraestructura y Aceptación del consumidor*. Estos se componen de variables que reflejan numerosos factores desde la disponibilidad de estaciones de carga de vehículos eléctricos y el ambiente regulatorio, hasta la I+D+i y la disposición de la población a adoptar tecnología.

El AVRI destaca algunos atributos que tienen los países más preparados, además de un sólido desarrollo económico, como:

- Gobiernos dispuestos a regular y apoyar el desarrollo de vehículos autónomos.
- Excelente infraestructura de carreteras y redes móviles.
- Inversión e innovación del sector privado.
- Pruebas a gran escala impulsadas por una fuerte presencia de la industria automotriz.
- Un gobierno proactivo que atrae alianzas con los fabricantes.

I.1.5 Un ciclo de actualización más corto de los modelos

En el nuevo mercado al que nos encaminamos, los tradicionales ciclos de actualización de los modelos de, entre cinco y ocho años, se convertirán en algo del pasado. En su lugar, los fabricantes apostarán por realizar actualizaciones anuales de su porfolio de modelos para incorporar los últimos desarrollos tanto de hardware como de software.

[25] KPMG INTERNATIONAL, 2019. 2019 Autonomous Vehicles Readiness Index. [en línea]. Ginebra, Suiza: KPMG International. [Consulta: 25 marzo 2019]. 136024-G. Disponible en: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf.
[26] Ver Anexo No. 2 al presente trabajo.

I.2 Irrupción de las TIC en el sector del automóvil y la afinidad de dos mundos

La tecnología del automóvil y las tecnologías de la información y la comunicación (TIC) están convergiendo a un ritmo creciente. Las empresas, los consumidores y los planificadores urbanos, están beneficiándose paulatinamente de muchas maneras, desde el crecimiento de la nueva industria hasta una mayor seguridad en las vías; mientras toda una gama de soluciones para las ciudades inteligentes como son los sistemas de transporte inteligentes, que comienza a reducir la congestión del tráfico y a incrementar la conectividad y movilidad de los habitantes de las ciudades[27].

En España, por ejemplo, a finales del año 2015, la Dirección General de Tráfico (DGT)[28] del Ministerio del Interior aprobó una primera normativa[29] que permite la prueba de vehículos autónomos por las carreteras españolas. Un vehículo que cubrió la ruta de Vigo a Madrid fue el primero en probar esta tecnología, se realizó utilizando un Citroën C4 Picasso, equipado para ajustar la velocidad por sí mismo y decidir en qué momento debía adelantar a otros vehículos durante el viaje[30].

La existencia de legislación para este tipo de pruebas no imposibilita que un particular pueda circular en España con un vehículo que se conduzca solo. España, que no se ha adherido a la Convención de Viena sobre Circulación Vial firmada en 1968, no está sujeta a ciertas limitaciones, que sí tienen otros países del entorno europeo. Esta situación ya ha provocado las quejas de otros estados miembros de la Unión, que no pueden desarrollar una tecnología que debería entrar en vigor en muy pocos años[31].

---

[27]ZHAO, HOULIN; LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN; FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.

[28] El Real Decreto 2822/1998 de 23 de diciembre, por el que se aprueba el Reglamento General de Vehículos (RGV), otorgó en su artículo 47 a la Dirección General de Tráfico la facultad de concesión de autorizaciones especiales para la realización de pruebas o ensayos de investigación extraordinarios, realizados por fabricantes, fabricantes de segunda fase y laboratorios oficiales.

[29] Instrucción No. 15/V-113 de la Dirección General de Tráfico del Ministerio del Interior, de 13 de noviembre de 2015, sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general.

[30] ESTEVE, J., 2016. España se pone las pilas: la DGT regulará por primera vez el coche autónomo en 2017. *El Confidencial* [en línea]. [Consulta: 14 junio 2019]. Disponible en: https://www.elconfidencial.com/tecnologia/2016-12-23/coche-autonomo-espana-dgt-2017-reglamento_1308238/.

[31] CANO, V., 2019. Las 6 tendencias en el automóvil que marcarán 2019. [en línea]. [Consulta: 25 marzo 2019]. Disponible en: https://www.autobild.es/listas/6-tendencias-automovil-que-marcaran-2019-349119

Que en España ya se puede conducir un Tesla con el modo "autopiloto", es sólo una de las ventajas que tienen los conductores de vehículos con diferentes grados de automatización en este país[32]. La DGT en el mes de marzo de 2016, aprobó mediante otra normativa[33] el aparcamiento automático o asistido, por el que un conductor puede salir del coche mientras este se estaciona solo.

A nivel del parlamento nacional resulta un referente la Proposición no de Ley que fuera presentada por el Grupo Parlamentario Popular en el Congreso, sobre el impulso y desarrollo del vehículo autónomo (núm. expediente 162/000451)[34], aprobado por el Pleno del Congreso de los Diputados en su sesión del día 10 de octubre de 2017.

A nivel autonómico se puede mencionar[35] a la Comunidad de Castilla y León, que ha dispuesto normativamente que las administraciones impulsarán el despliegue e implantación de estrategias de movilidad automatizada y conectada, que aumenten la eficiencia y la seguridad de transporte público de viajeros por carretera, mejoren los flujos de tráfico en la infraestructura vial y de comunicaciones y reduzcan los impactos medioambientales; a su vez, que de conformidad con lo establecido por la regulación estatal en materia de tráfico y seguridad vial, estas promoverán la realización de pruebas

[32] ESTEVE, J., 2016. España se pone las pilas: la DGT regulará por primera vez el coche autónomo en 2017. *El Confidencial* [en línea]. [Consulta: 14 junio 2019]. Disponible en: https://www.elconfidencial.com/tecnologia/2016-12-23/coche-autonomo-espana-dgt-2017-reglamento_1308238/.

[33] Instrucción No. 16 TV/89 de la Dirección General de Tráfico del Ministerio del Interior, de 20 de enero de 2016, sobre la autorización del uso de los sistemas de estacionamiento asistido de vehículos a motor para emplearse en las vías abiertas al tráfico.

[34] En esta proposición el Congreso de los Diputados insta al Gobierno a:
1. Promover el desarrollo del vehículo autónomo evaluando el funcionamiento de la actual legislación específica e identificando posibles mejoras en la misma, que impulsen la realización de investigación y desarrollo, así como validación de prototipos.
2. Impulsar el desarrollo del sector del automóvil, así como el ecosistema de empresas y Pymes altamente innovadoras asociadas a la fabricación del automóvil y a la creación de empleo de calidad, todo ello complementado con programas de I+D+i para el sector.
3. Desarrollar medidas que fortalezcan la competitividad industrial del automóvil en nuestro país facilitando su transición hacia las necesidades del vehículo autónomo, fomentando la especialización y cualificación del empleo asociado a las nuevas necesidades tecnológicas de esta nueva industria.
4. Fomentar acciones que permitan la consolidación de España como referente mundial para las pruebas del vehículo autónomo conectado, asistido y semiautónomos y en todos sus niveles. Evaluando también el impacto social y medioambiental del desarrollo de esta industria."

[35] Este y los anteriores ejemplos de la nación ibérica demuestran como dos industrias tan diferentes han encontrado vías de colaboración para extender los beneficios de la innovación del automóvil conectado a todos de manera segura y a su vez muchas entidades del sector público se han trazado el objetivo de coadyuvar su desarrollo de manera efectiva.

y ensayos de investigación con vehículos autónomos en las vías urbanas e interurbanas abiertas al tráfico[36].

Ante todo, el automóvil se ha convertido en un navegador sobre ruedas por lo que resulta difícil exagerar este fenómeno que viene a significar, que conducir se ha convertido en sinónimo de buscar en línea (un sector cuyo valor supera los 100 000 millones de dólares), con todo lo que esto implica para rentabilizar el comportamiento al volante, pues todos los gestos o acciones de un conductor indican intenciones y conductas que generan potenciales beneficios para publicistas y fabricantes de automóviles[37].

Actualmente, la plataforma Marketplace de General Motors es el ejemplo perfecto de un sistema integrado en el vehículo que hace recomendaciones en tiempo real al conductor directamente desde el salpicadero, a partir de análisis predictivos basados en las preferencias del cliente y su comportamiento anterior[38].

Las redes inalámbricas tendrán también un papel fundamental para luchar contra las amenazas a la ciberseguridad y ofrecer actualizaciones de mapas en tiempo real para la conducción automática, así como actualizaciones de software para los sistemas integrados esenciales y para los demás; sin embargo, en general, el cambio más significativo en la conectividad a bordo tendrá lugar cuando la industria automovilística reconozca y acepte que la red inalámbrica tiene un papel clave para la seguridad de los vehículos[39].

[36] Tal como se expresa en el artículo 20 de la Ley 9/2018, de 20 de diciembre, de transporte público de viajeros por carretera de Castilla y León, emitida por las cortes de la referida comunidad autónoma.
[37] ZHAO, HOULIN; LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN; FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.
[38] Ídem
[39] Ibidem.

La primera manifestación de esta realidad, la tecnología C-V2X[40], es una auténtica revolución que nos acerca a una Internet de las Cosas (IoT por sus siglas en inglés) completamente integrada en el vehículo[41].

I.3 La inteligencia artificial y los vehículos

Los vehículos autónomos guiados por inteligencia artificial posibilitarán la transición hacia la movilidad como servicio en los próximos años y décadas. La producción de gases de efecto invernadero en el transporte urbano puede reducirse considerablemente mediante la optimización del tráfico y de las rutas, los algoritmos de conducción ecológica, la agrupación de vehículos en trenes de carretera y los servicios de transporte compartido en vehículos autónomos. Las flotas de vehículos eléctricos autónomos serán fundamentales para lograr auténticos beneficios[42].

El fenómeno de los navegadores se está acelerando con el cambio de las capacidades de la inteligencia artificial, que facilitan la conducción automatizada y los asistentes digitales. Se pasa así de la nube a sistemas integrados en el vehículo, con procesadores más potentes, redes de vehículos mejoradas y almacenamiento a bordo. Los automóviles cada vez entienden mejor lo que hacen los humanos y les ayudan a desplazarse y llegar a su destino de forma segura y precisa[43].

---

[40] Estos microcircuitos celulares denominados Vehicle-to-Everything (C-V2X) completarán el ecosistema de los coches conectados mejorando cobertura, fiabilidad, velocidad, asistencia y rentabilidad. Qualcomm, empresa líder en la producción de semiconductores y equipos de telecomunicaciones invierte cada vez más en este tipo de proyectos para el sector automovilístico. La tecnología móvil también desempeña una función esencial en los sistemas de transporte inteligente (ITS por sus siglas en inglés) al proporcionar estos servicios celulares de Vehículo-a-Todo (C-V2X). Estandarizado por 3GPP, C-V2X admite la conectividad entre dispositivos (ya sea en vehículos, infraestructura vial o dispositivos móviles) y entre dispositivos y redes. C-V2X se está desarrollando dentro del ecosistema móvil tradicional y reúne todas las ventajas y capacidades que ofrecen las redes celulares de comunicación tradicionales: seguridad, privacidad, interoperabilidad y un ecosistema orientado a la innovación, compatible con el futuro (tecnología 5G). La Asociación Automotriz 5G (5GAA), cuyos 60 miembros incluyen a los principales fabricantes de vehículos, admiten C-V2X.

[41] Como expresan muchos expertos resulta fascinante imaginar lo que nos queda por ver, en tan solo unos años, con la aparición de la 5G; debido a que en un momento crítico de la evolución del sector de las redes inalámbricas, la industria automovilística colabora con la de las telecomunicaciones para desarrollar normas y protocolos acordados por ambos.

[42]ZHAO, H. y VECCHIONE, MAURIZIO; HERWEIJER, CELINE; STEWART, UYI; IBARAKI, STEPHEN; ZURUTUZA, NAROA; SAHOTA, NEIL; FENECH, MATTHEW; SALIBA, T., 2018. Inteligencia artificial para el bien del mundo. *ITU News Magazine* [en línea]. Ginebra: Unión Internacional de Telecomunicaciones. [Consulta: 14 junio 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-01/2018_ITUNews01-es.pdf.

[43] La compañía HERE Technologies por ejemplo, posee hasta la fecha 13 productos o soluciones para vehículos conectados y autónomos relacionados con inteligencia artificial, y trabaja en este momento para

I.4 Servicios de telecomunicaciones y su provisión por la industria automovilística

En el marco de esta transformación que está acaeciendo en su sector, los fabricantes automovilísticos plantean convertirse en operadores de redes móviles virtuales autónomos, para desarrollar un modelo de negocio alejado o diferenciado de los operadores de telecomunicaciones dominantes en estos mercados; estos desean que sus vehículos puedan acceder a las mejores conexiones inalámbricas en cualquier lugar, sea cual sea el proveedor del servicio.

La conectividad va a ser importante para la diferenciación entre los fabricantes de automóviles y operadores, como Transatel[44]; para estos fabricantes va a formar parte de su núcleo de negocio el convertirse en Operadores Móviles Virtuales (OMV), ya que necesitan controlar las medidas de seguridad y la diferenciación del servicio, y hacerlo de manera homogénea en todo el mundo. Se presenta una gran oportunidad para que los OMV ofrezcan servicios a la industria del automóvil, así como para los fabricantes de equipos de telecomunicaciones, ya que algunos fabricantes de automóviles querrán invertir en la práctica en la infraestructura de telecomunicaciones[45].

Esta oportunidad también se presenta en el contexto actual y futuro para los operadores móviles, pues se utilizarán muchos más datos en sus redes, por lo que es también una gran oportunidad para que desarrollen la red, ya sea 3G o 4G y, mañana, 5G, y lograr una utilización muy superior a la existente actualmente, dado que los vehículos van a utilizar un enorme volumen de datos[46].

integrar la información sobre ubicaciones de la navegación con información contextual obtenida por sensores y recopilada por vehículos de Audi, BMW y Daimler para ayudar a los conductores a evitar en su camino obstáculos y peligros de la carretera.

[44] Los fabricantes de automóviles están explorando nuevos programas de cooperación, redefiniendo su visión del propio sector; un ejemplo de esto es la compañía Transatel, sociedad que ofrece soluciones de conectividad para que las empresas ajenas al sector de las telecomunicaciones se conviertan en operadores de redes móviles virtuales y ofrezcan sus redes propias.

[45] Según declaró Jacques Bonifay, Director Ejecutivo de Transatel (un miembro de la UIT) y Jefe de la Asociación de Operadores de Red Móvil Virtual de la Unión Europea, en una entrevista concedida a ITU News durante su presencia y participación en el Simposio UIT/CEPE sobre el vehículo conectado del futuro 2018.

[46] Ídem.

CAPÍTULO II - LA ACTIVIDAD DE LOS GOBIERNOS EN UN ENTORNO DE TRANSFORMACIÓN DIGITAL

II.1 La gestión de los gobiernos en un entorno de transformación digital

El proceso de transformación digital incluye una serie de propensiones de desarrollo como las ciudades inteligentes, la inteligencia artificial, la Internet de las Cosas o el Internet del Todo (IoE por sus siglas en inglés[47]) como su etapa más avanzada; todo lo cual es considerado como la nueva revolución industrial, económica y social. Estos fenómenos están cambiando nuestras vidas. Todos los objetos o los elementos vivos que forman parte de la vida cotidiana de los seres humanos; desde las mascotas o animales de trabajo[48] o recreo, hasta el coche pasando por los objetos del ámbito doméstico y los aparatos médicos, de una forma u otra estarán conectados a Internet u otro tipo de red de infocomunicación, mediante enlaces máquina a máquina, de persona a máquina y de persona a persona[49].

La situación expuesta implica que los estados tanto en sus estructuras centrales como locales, se aseguren de estar preparados para los desafíos que plantea este movimiento de origen tecnológico; pero que marcan todos los aspectos de la vida, por lo que han emprendido mecanismos de innovación[50] de la gestión pública que han implicado una

[47] Como ejemplo de la definición podemos utilizar la que CISCO Networking Academy expresara en un resumen del curso sobre introducción al Internet que organizara en 2014 y donde se definía que el Internet del Todo (IoT) reúne a las personas, los procesos, los datos y los objetos para lograr que las conexiones en red sean más relevantes y valiosas que nunca mediante la transformación de la información en acciones que, a su vez, creen nuevas funcionalidades, mejores experiencias y oportunidades económicas sin precedentes para empresas, individuos y países.

[48] Por ejemplo, en China se acomete el Connected Cow, que es un innovador proyecto realizado en una granja lechera con más de 50,000 vacas en la ciudad de Yinchuan, desarrollado por las compañías China Telecom, Huawei y Aotoso, el "Pequeño Pastor" sistema de nube de detección de oestro de vaca adopta NB-IoT. El sensor NB-IoT amarrado al cuello de cada vaca puede medir su temperatura corporal para garantizar su seguridad mientras se detecta oestro para el apareamiento oportuno. Además de las vacas, el sistema también se aplicará en granjas de carne, empresas de lácteos y las asociaciones de ganadería. China Telecom comenzó el despliegue del sensor NB-IoT para las 50,000 vacas, y deben llegar a 1.2 millones. Los estudios recientes muestran que con más de 1300 millones de cabezas de ganado vacuno en todo el mundo, existe una gran demanda de soluciones innovadoras de IoT como "Pequeño Pastor" en la industria.

[49] Palabras del Sr. Sorin Grindeanu, presidente, de la agencia ANCOM de Rumania, durante el Simposio Mundial para Organismos Reguladores de las Telecomunicaciones 2018 –ITUGSR Geneva 2018.

[50] Según expresa el Instituto Nacional de Administración Pública de España en su sitio web institucional, una administración pública moderna, ágil y eficiente es determinante para lograr una sociedad con mayores cotas de bienestar y de calidad de vida; para lograr alcanzar estas metas, la administración actual necesita creatividad e innovación. La administración pública debe asumir un rol ejemplar de liderazgo con respecto a la innovación, a través de la mejora de los servicios públicos, la orientación a la ciudadanía y a las empresas y la eficiencia operativa, entre otros. En este sentido, procede desarrollar el concepto de

mayor participación y colaboración en la toma de decisiones públicas[51], de múltiples actores de la sociedad, que den respuesta a los grandes desafíos venideros.

Los gobiernos establecen entonces enfoques políticos y normativos anticipadores, basados en la colaboración y dinámicos, junto a unos modelos innovadores y sostenibles de gestión pública de facilitación de los negocios y la inversión, indispensables para crear las condiciones que permitan que esta transformación desarrolle todo su potencial. Al mismo tiempo, existe una necesidad permanente de una infraestructura acreditada, segura y fiable, así como de un acceso y una prestación asequibles en lo que respecta a los servicios digitales[52].

II.2 La actividad de los gobiernos y la Internet de las Cosas

El mercado de la Internet de las Cosas (IoT)[53] se está desarrollando a gran velocidad[54] y con el avance de la más reciente generación de tecnología de comunicación móvil celular terrestre o 5G, con sus características de baja latencia y seguridad[55] jugarán un papel muy

innovación pública, entendido como la aplicación de ideas y prácticas novedosas en el ámbito de la gestión pública con el objetivo de generar valor social.

[51] En España como ejemplos de creación de plataformas abiertas, transparentes y colaborativas de participación ciudadana en la toma de decisiones pueden mencionarse a "Decide Madrid" o "Decidim Barcelona".

[52] ZHAO, HOULIN; IBARAKI, STEPHEN; SAHOTA, NEIL; NARAIN, NIVEN R.; AKHTMAN, JOSEF; KHALDI, NORA; BROWNE, EMMET; HINCHEY, MIKE; WERNER, FREDERIC; BANIFATEMI, A., 2018. Nuevas fronteras reglamentarias. Cómo las tecnologías emergentes están dando lugar a enormes oportunidades y desafíos potenciales. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 24 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-03/2018_ITUNews03-es.pdf.

[53] El IoT, más específicamente, podría ser entendido como un sistema en el que la totalidad de los dispositivos (infraestructuras, vehículos, máquinas y otros elementos electrónicos) están interconectados gracias a varias o a la misma red para generar y compartir datos.

En 2013, la "Global Standards Initiative on Internet of Things" (IoT-GSI) definió el IoT como una infraestructura global para la sociedad de la información que permita servicios avanzados interconectando "cosas" (física y virtualmente) basadas en tecnologías de la información y la comunicación tanto existentes como en evolución. Entendiendo como "cosas" todo objeto físico o perteneciente al mundo de la información (objeto virtual), capaz de ser identificado e integrado en una red de comunicaciones. En ese sentido puede consultarse la Recomendación UIT-T Y.2060 Descripción general de Internet de los objetos.

[54] De acuerdo con las cifras de la GSMA; al cierre de 2018 el número de dispositivos conectados alcanzó la cifra de 9100 millones (de ellos 1200 millones de vehículos conectados), estimándose que en el 2025 sean 252 000 millones. En el caso de las conexiones celulares de la IoT alcanzó los 760 millones en 2018, cifra que se disparará hasta casi sobrepasar los 3100 millones en 2025. Resulta comprensible que los gobiernos tengan cada vez más interés en aprovechar los beneficios de la IoT y canalizarlos hacia los ciudadanos.

[55] Un vehículo autónomo operado a través de un sistema de conducción autónomo basado en la nube debe poder detenerse, acelerar o girar cuando se le indique que lo haga. Cualquier latencia o pérdida de la cobertura de la señal en la red que impida que el mensaje se entregue podría tener consecuencias

importante en la evolución de los sistemas de transporte inteligentes, permitiendo que los vehículos inteligentes se comuniquen entre sí, creando oportunidades para automóviles y camiones conectados y autónomos[56].

Los fórums tecnológicos y organismos de estandarización ponen de relieve requisitos tecnológicos y económicos principales previstos para el despliegue masivo de servicios de IoT[57].

La IoT promete ofrecer un gran número de beneficios para los ciudadanos, los consumidores, las empresas y los gobiernos, por el enorme potencial que posee para reducir los costos sanitarios y de educación, reducir las emisiones de carbono, aumentar el acceso a la educación, mejorar la seguridad en el transporte y mucho más.

Los gobiernos a fin de aprovechar estos beneficios deben crear políticas que proporcionen los incentivos adecuados para el crecimiento y la innovación[58]; apoyando y promoviendo especificaciones y estándares interoperables para todo el sector de la IoT, incluida la adopción de soluciones de la IoT en el sector público o financiando programas de investigación y desarrollo[59].

Dado que el ecosistema de la IoT está compuesto por un gran número de agentes o actores diferentes, los marcos legales se deben basar en una regulación justa para servicios equivalentes, donde es muy importante la claridad en las regulaciones para ofrecer a los

---

catastróficas. Los operadores inalámbricos creen que los vehículos autónomos tienen un camino importante antes de que entren en servicio, a pesar de los ensayos y pilotos en curso.

[56] En el Reino Unido se otorgó una subvención gubernamental de 17,6 millones de libras esterlinas a un consorcio liderado por la Universidad de Warwick para desarrollar un banco de pruebas central para vehículos autónomos conectados. Las celdas pequeñas se desplegarán a lo largo de una ruta donde se probarán a través de las ciudades de Coventry y Birmingham.

[57] Estos requisitos son: dispositivos de bajo coste, se necesita que estén integrados, no solo en un modem de un chip, sino también con sensores y actuadores; sistemas de gestión eficiente de energía, que permitan la mayor autonomía a los dispositivos IoT y cobertura ubicua en el escenario de despliegue. El despliegue realizado debe garantizar un alto grado de cobertura, sobre todo en interiores, pero también en exteriores y; escalabilidad, teniendo en cuenta el alto número de dispositivos que entrarán en juego en los despliegues de los escenarios "ultra-densos" y el crecimiento exponencial de los dispositivos.

[58] Esto es importante para el futuro crecimiento de la IoT, ya que las plataformas y los servicios interoperables, como las que se utilizaran como soporte de los sistemas de gestión de vehículos autónomos, reducen los costos de despliegue y su complejidad, facilitan la escalabilidad y permiten que los consumidores puedan disfrutar de experiencias conectadas a nivel global intuitivas y de similares características al contratado en el lugar de origen.

[59] GSMA, 2019. *Manual de Políticas Públicas de Telecomunicaciones Móviles. Una guía de temas clave.* [en línea]. S.l.: s.n. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

proveedores de servicios y fabricantes de dispositivos para la IoT la confianza y seguridad jurídica que necesitan para invertir en esta tecnología emergente a escala global[60].

II.3 Robótica e inteligencia artificial y la intervención de los gobiernos

Un robot[61] es una máquina, provista de cierta complejidad tanto en sus componentes como en su diseño o en su comportamiento, y que manipula información acerca de su entorno para así interactuar con él. La robótica[62] híbrida de los vehículos inteligentes abarca todos aquellos componentes[63] electromecánicos, hidráulicos, electrónicos, de hardware o de software que tras su mejora progresiva e incremental por diferentes actores tecnológicos que se han ido introduciendo en el sector del automóvil; ha ido convirtiendo a estos apreciados y muy utilizados objetos en computadoras con ruedas conectadas a diversas redes mediante disímiles tecnologías de conectividad para aprovechar todas sus capacidades.

La Inteligencia Artificial[64], entendida como la simulación de procesos de inteligencia humana en máquinas[65], tiene un poder transformador de la sociedad que sin embargo conlleva retos difíciles, que van desde cuestiones éticas hasta problemas de seguridad, pasando por los efectos negativos que puede tener sobre el empleo.

En aras de poder allanar el camino de un futuro basado en la inteligencia artificial, se considera que los países utilizando un modelo consensuado de múltiples partes

[60] GSMA, 2019. *Manual de Políticas Públicas de Telecomunicaciones Móviles. Una guía de temas clave*. [en línea]. S.l.: s.n. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

[61]BARRIO ANDRÉS, M., ARANSAY ALEJANDRE, A., DOMÍNGUEZ PECO, E., GARCÍA PORTERO, R., GARCÍA-PRIETO CUESTA, J., GÓMEZ-RIESCO TABERNERO DE PAZ, J., SEGURA ALASTRUÉ, M. (2018). *Derecho de los Robots* (Primera Edición ed.)., Madrid, España: Wolters Kluwer España, S.A.

[62] Según el Diccionario de la Lengua Española que publica la Real Academia de la Lengua, robótica es la técnica que aplica la informática al diseño y empleo de aparatos que, en sustitución de personas, realizan operaciones o trabajos, por lo general en instalaciones industriales.

[63] Ver Anexo No. 3 al presente trabajo.

[64] La Inteligencia Artificial responde básicamente a la idea de robots; abarcando la recopilación de datos, la toma de decisiones y las acciones correctivas que se realizan de forma automatizada mediante la robótica para poder detectar problemas, programar acciones, y por lo general, optimizar los insumos y la rentabilidad de casi cualquier actividad humana hasta el presente. Su utilización permite aumentar la efectividad en la utilización de recursos, reduciendo su consumo y causando menos daño a importantes ecosistemas.

[65] DELOITTE. (2017). *Inteligencia de máquina: La tecnología imita el conocimiento humano para crear valor.* Deloitte University Press.

interesadas[66], deben atender determinas premisas, tales como[67]: reforzar el papel que desempeña el ser humano, propugnando un código ético propio para estas tecnologías y garantizar el diálogo, las normas prácticas y los métodos óptimos en su desarrollo y utilización; fomentar la reglamentación y la supervisión inteligente y oportuna, que asegure que el camino del cambio tecnológico va acompañado de una respuesta igualmente rápida en materia de reglamentación[68], con políticas que destaquen y potencien los beneficios tangibles de la inteligencia artificial, así como la repercusión positiva para todas las personas; y potenciar su accesibilidad a todo el mundo por igual, para garantizar que todas las personas tengan acceso a las herramientas innovadoras, los datos y la tecnología de la manera más democrática posible.

Ocuparse de estos desafíos puede resultar tan difícil, si no se abordan por los gobiernos con una colaboración sin precedentes con todas las empresas, las instituciones académicas y los individuos para poder considerar y gestionar los riesgos que se estiman se produzcan, a partir de su progresiva introducción a nivel exponencial en la vida cotidiana.

[66] Esa es la razón por la que se han creado nuevas iniciativas que incluyen a los sectores público y privado para fomentar la IA en beneficio de toda la humanidad. Por ejemplo, Open AI, Partnership on AI y el Concurso AI XPRIZE, se centran en los beneficios de la IA para el ser humano proponiendo que la IA sea una extensión de las capacidades de las personas, ampliamente accesible y distribuida lo máximo posible. El concurso IBM Watson AI XPRIZE, que anualmente desde 2026 convoca a cientos de equipos de distintos países que se enfrentan a los retos más importantes del mundo utilizando aplicaciones de IA para abordar los 17 Objetivos de Desarrollo Sostenible.

[67]ZHAO, H., IBARAKI, S., SAHOTA, N., NARAIN, N. R., AKHTMAN, J., KHALDI, N., BANIFATEMI, A. (2017). *AI para el bien social. Cómo puede la inteligencia artificial impulsar el desarrollo sostenible.* Unión Internacional de Telecomunicaciones. Ginebra: ITU News.

[68] La cumbre anual AI for Good, que se realiza y organiza en el marco de la Unión Internacional de Telecomunicaciones, agencia intergubernamental del sistema de las Naciones Unidas; se ha convertido en una plataforma donde los diversos interesados a nivel mundial crean redes de colaboración en materia de IA a nivel internacional y en diversas disciplinas. Los participantes en la cumbre debaten cómo puede ser la IA el motor de un cambio positivo, para promover la democracia, erradicar la pobreza, permitir y fomentar la innovación para todos por igual y adoptar principios rectores que ayuden a sentar las bases para el futuro del ser humano y las máquinas.

CAPÍTULO III - ROL DE LOS GOBIERNOS EN LA GARANTÍA DEL DESARROLLO Y ADOPCIÓN DE FORMA SEGURA DE LOS VEHÍCULOS INTELIGENTES

III.1 El proceso de normalización técnica de los vehículos inteligentes

III.1.1 Aspectos generales

Los vehículos inteligentes[69] se consideran automatizados y autónomos cuando al menos algún aspecto de una función de control de seguridad crítica (dirección, aceleración o frenado) se produce sin la entrada directa del conductor. Los vehículos automatizados pueden ser autónomos y conectados cuando se emplean sistemas de comunicaciones en la que los autos y la infraestructura vial o de gestión del sistema de transporte se comunican de manera inalámbrica. La conectividad es un insumo importante para obtener los beneficios potenciales completos y la implementación a gran escala de vehículos automatizados.

Debido a que su utilización es global, la normalización técnica o estandarización[70] va a ser esencial para elaborar un ecosistema seguro de vehículos inteligentes con estándares lo más homogéneo posible en todos los países[71]; que facilite la integración creciente de las tecnologías de la información y la comunicaciones en los vehículos con la seguridad vial, la protección de datos personales y la interoperabilidad como capacidad de los sistemas y de los procesos empresariales subyacentes para intercambiar datos y compartir información y conocimientos.

[69] Como hemos explicado los vehículos inteligentes abarcan una gama de automóviles que forman parte de sistemas de transporte inteligentes; en los que para su automatización se conjugan las telecomunicaciones (vehículos conectados) y diferentes tecnologías de la información y las comunicaciones en el ámbito del transporte por carretera, que pueden conformarse en apoyo de la labor de conducción (ADAS) o como verdaderos sistemas operativos avanzados con capacidad de autoconducción (semiautónoma o totalmente autónoma) , así como para las interfaces con otros modos de transporte.

[70] El debate en curso sobre este proceso es sobre si los gobiernos deben intervenir y determinar los estándares y la tecnología a utilizar en los vehículos inteligentes, o si deben dejar abierta la normalización técnica a los desarrollos, la voluntariedad o la autorregulación de la industria automovilística tanto de los actores tradicionales como no tradicionales.

[71] Durante el Simposio sobre los vehículos conectados del futuro celebrado el 8 de marzo de 2018 (FNC-18), reunión anual organizada por la UIT y la Comisión Económica de las Naciones Unidas para Europa (CEPE) en el marco del Salón del Automóvil de Ginebra; David Wong, director de tecnología e innovación de la Asociación de Fabricantes y Comerciantes de Motores del Reino Unido, expresó también que los reglamentos, políticas y normas son, en su opinión, una de las cuatro dificultades para el desarrollo de vehículos conectados.

Al ser parte los vehículos inteligentes del entorno del Internet de las Cosas, a su proceso de normalización técnica, le es aplicable las variadas iniciativas globales de estandarización que tratan de impulsar el desarrollo de un IoT eficiente, escalable y seguro; donde los esfuerzos se centran en estandarizar las redes de conectividad sustentadoras de las distintas soluciones IoT, regular la gestión de los dispositivos que entran en juego en dichas soluciones, generar arquitecturas de referencia y herramientas normalizadoras y garantizar la seguridad y la privacidad de los datos a lo largo de toda la arquitectura[72].

Organizaciones de estandarización, alianzas industriales y grupos de interés en el IoT están creando estándares y arquitecturas de referencia para las diferentes capas de la pila de tecnología IoT. A continuación, se verán las soluciones más relevantes, a excepción de las relacionadas con política y reglamentación, ciberseguridad y privacidad de datos personales, en las que nos centraremos en secciones posteriores.

III.1.2 Unión Europea y España

La Unión Europea ha fijado como un principio general[73], que las normas técnicas de los vehículos e infraestructuras (por ejemplo, señales de tráfico, marcas viales, sistemas de señalización y sistemas de transporte inteligente cooperativos) deberían desarrollarse y armonizarse a escala nacional, internacional y de la Unión, partiendo de los trabajos y foros ya existentes para evitar solapamientos, sobre la base de los principios de un enfoque abierto, transparente y tecnológicamente neutro, aumentando la seguridad vial y garantizando una interoperabilidad transfronteriza completa.

Mediante la Directiva (UE) 2010/40 del Parlamento Europeo y del Consejo de 7 de julio de 2010, fue establecido el marco para la implantación de los sistemas de transporte

[72] DELOITTE, 2018. IoT para el Sector Empresarial en América Latina. En: DELOITTE (ed.) [en línea]. Uruguay: Centro de Estudios de Telecomunicaciones de América Latina. [Consulta: 16 marzo 2019]. Disponible en: https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/.
[73] Resolución del Parlamento Europeo, de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos (2018/2089(INI)).

inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte[74].

En el contexto español se debe resaltar el procedimiento aprobado[75] vinculado a la obtención del certificado para la realización de pruebas de conducción autónoma, emitido por un servicio técnico acreditado[76]; según los procedimientos recogidos en el anexo II de la disposición normativa, mediante la cual fue aprobado, o acreditación de haber obtenido previamente, de la autoridad competente de otro Estado Miembro de la Unión Europea, a través de un procedimiento de control previo equivalente.

III.1.3 Estados Unidos de América

El Departamento de Transporte de los EUA (US DOT por sus siglas en inglés) ha establecido un enfoque claro y coherente para la configuración de la política federal del país sobre vehículos automatizados[77], basada en seis principios fundamentales[78]; como uno de estos principios se encuentra, la modernización o eliminación de las reglamentaciones obsoletas que impiden innecesariamente el desarrollo de vehículos automatizados o que no abordan necesidades críticas de seguridad.

---

[74] Específicamente en su artículo 8.1 se dispuso que: *"Las normas necesarias para proveer la interoperabilidad, compatibilidad y continuidad de la implantación y explotación operativa de los sistemas de transporte inteligente serán desarrolladas en los ámbitos prioritarios y para las acciones prioritarias. A tal fin, la Comisión Europea, una vez consultado el comité mencionado en el artículo 15 de esta propia directiva, solicitará a los organismos de normalización correspondientes, de conformidad con el procedimiento establecido en la Directiva 98/34/CE[74], que haga cuanto sea necesario para la rápida adopción de esas normas".*

[75] Instrucción No. 15/V-113 de la Dirección General de Tráfico del Ministerio del Interior, de 13 de noviembre de 2015, sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general.

[76] Estos servicios técnicos pueden emitir esta certificación, luego de haber demostrado mediante la presentación de una solicitud de acreditación a la Entidad Nacional de Acreditación (ENAC) designada por el Gobierno, para operar en España como el único Organismo Nacional de Acreditación, incluyendo una declaración responsable que le acrediten disponer de las competencias técnicas para la ejecución de las actividades que se recogen en el procedimiento de certificación.

[77] U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

[78] Estos 6 principios para la configuración de la política federal de EUA sobre vehículos automatizados están relacionados con: dar prioridad a la seguridad, seguir siendo tecnológicamente neutrales, modernizar las regulaciones, fomentar un entorno regulatorio y operativo consistente, preparar de forma proactiva la automatización así como proteger y mejorar las libertades de las que disfrutan los ciudadanos estadounidenses.

El Departamento de Transporte de los EUA ha indicado que siempre que sea posible, apoyará programas de desarrollo de estándares técnicos basados en el consenso y la aceptación voluntaria, y enfoques flexibles y adaptables a lo largo del tiempo.

III.1.4 China

Un hito fundamental en materia de estandarización de los vehículos inteligentes en este país lo marca el 29 de diciembre de 2017; fecha en la que el Ministerio de Industria y Tecnología de la Información (MIIT) y la Administración de Normalización (SAC) de la República Popular China, emitieron conjuntamente las ***"Guideline for Developing National Internet of Vehicles Industry Standard System Intelligent & Connected Vehicle)***[79]. Esto sucedió seis meses después de que, para consulta el borrador de las directrices, se publicara el 13 de junio de 2017. Estas directrices tienen como objetivo establecer estándares o normas técnicas nacionales para los vehículos inteligentes y conectados[80].

En las directrices se establece que el sistema este compuesto por 99 normas técnicas, incluyendo 11 básicas, 31 para especificación general, 49 para aplicación en productos y tecnologías y 8 para normas relevantes o relacionadas. Este sistema de normas juega un papel importante en el desarrollo de la industria de los vehículos inteligentes y conectados de China[81].

---

[79] Este esfuerzo forma parte del proceso de implementación del Plan Estratégico "Hecho en China 2025", por parte del gobierno de esta nación; basados en el rol que poseen los estándares en facilitar la promoción del desarrollo tecnológico e industrial de sistemas inteligentes y conectados, y lograr una alta integración de la industrialización y la información de la información, a fin de satisfacer las necesidades de I+D+i. Con este documento se pretende igualmente fomentar la realización de pruebas, demostraciones y operaciones, para promover la innovación y el desarrollo de la tecnología automotriz, la transformación y modernización industrial; el desarrollo coordinado de las industrias de la información, la electrónica, las comunicaciones y otras relacionadas; para construir una futura sociedad automotriz segura, eficiente, saludable e inteligente, mediante un sistema estándar ICV que sea transversal y consistente con el desarrollo tecnológico e industrial.

[80] SCHAUB, M. y ZHAO, A., 2018. China Issues Final Guidelines on Standards Establishment for Self-driving Cars. *King & Wood Mallesons Law Firm Web* [en línea]. [Consulta: 11 junio 2019]. Disponible en: https://www.kwm.com/en/knowledge/insights/final-guidelines-on-standards-for-self-driving-cars-20180109#id-here.

[81] En particular, las Directrices finales incluyeron un nuevo párrafo en la sección de implementación en el que las autoridades analizarán cláusulas en las normas y reglas actuales relacionadas con la tecnología de los vehículos inteligentes y conectados y eliminarán gradualmente las normas y reglas que puedan impedir el desarrollo de nuevas tecnologías de este tipo para el sector de la industria automotriz, proporcionado un entorno de políticas sólido para su desarrollo.

III.1.5 Rusia

El 26 de noviembre de 2018, el gobierno de la Federación Rusa emitió un reglamento que permite que comiencen las pruebas de automóviles sin conductor en carreteras regulares. *(Gobierno de la Federación de Rusia, Reglamento Nº 1415, de 26 de noviembre de 2018, sobre la realización de un experimento para probar el uso de vehículos altamente automatizados en vías públicas).*

El gobierno ruso comenzó a realizar las pruebas experimentales[82] el 1 de diciembre de 2018 y estas abarcarán hasta el 1 de marzo de 2022 en carreteras de dos componentes principales de la Federación Rusa: la ciudad capital de Moscú y la República de Tatarstán, un territorio ubicado a unas 500 millas al este de la capital[83].

El gobierno simultáneamente aprobó las Reglas del experimento, designando un laboratorio de investigación gubernamental para coordinar las pruebas[84]. El laboratorio debe recopilar las solicitudes de los propietarios de los vehículos autónomos, emitir permisos de prueba después de revisar los vehículos de prueba y sus equipos electrónicos durante un período de revisión de 45 días, monitorear los resultados y proporcionar recomendaciones para los estándares de seguridad. Los informes que resuman los resultados de las pruebas y propongan los desarrollos adicionales, deben enviarse al gobierno en marzo de 2020 y nuevamente en 2022. Estos informes deben contener recomendaciones sobre requisitos técnicos y estándares para el uso práctico de vehículos autónomos[85].

[82] Durante el transcurso del experimento, en particular, prevé la confirmación de la posibilidad de operar un vehículo altamente automatizado en vías públicas en un modo de control automatizado y el desarrollo de requisitos técnicos para un sistema de conducción automatizado para el desarrollo de reglamentos técnicos y documentos de normalización. Basados en los datos obtenidos como resultado del experimento, se pretende determinar los requisitos a cumplir por los vehículos altamente automatizados durante la evaluación de la conformidad.

[83] BURANOV, I., 2018. Los coches sin conductor se hacen cargo. El gobierno libera drones a las carreteras de Rusia. *Kommersant.ru* [en línea]. [Consulta: 7 junio 2019]. Disponible en: https://www.kommersant.ru/doc/3792008.

[84] El Instituto Central de Automóviles y Automóviles de Investigación "NAMI" fue la entidad designada como el laboratorio de pruebas, donde se evaluará la evaluación de la conformidad de los requisitos de seguridad de los vehículos altamente automatizados.

[85] ROUDIK, P., 2019. Russia: Government Begins Testing Driverless Cars. *Library of the US Congress* [en línea]. [Consulta: 7 junio 2019]. Disponible en: https://www.loc.gov/law/foreign-news/article/russia-government-begins-testing-driverless-cars/.

III.1.6 Latinoamérica y el Caribe

En esta región por ejemplo; México se enfrenta a desafíos en legislación, tecnología e infraestructura para estar listo para la adopción de los vehículos inteligentes, debiéndose enfrentar actualmente a una serie de barreras, a la falta de regulaciones específicas y a la no realización de pruebas piloto activas de envergadura; sin embargo el proceso de integración económica con Canadá y los Estados Unidos de América debe forzar un proceso de armonización a los estándares tecnológicos que sobre los vehículos inteligentes han comenzado a implementarse en estos países.

En Brasil en términos de especificidad regulatoria, no se encuentran proyectos normativos en discusión, relacionados con los vehículos autónomos y particularmente sobre su estandarización técnica en el país; aunque un nuevo esquema de subsidios para el sector automotriz denominado "Plan Rota 2030"[86] que está siendo implementado por el gobierno, incluye algunos beneficios[87] que pueden incidir indirectamente con la estandarización de los vehículos inteligentes en el país.

Al ser básicamente receptores de tecnologías en algunos países latinoamericanos y caribeños[88]; ya se están implementado varias de estas en el sector del transporte por carretera, teniendo en cuenta los estándares comúnmente utilizados en otras regiones del planeta; sin embargo, dicha implantación en muchos casos se efectúa de forma

[86] MEDIDA PROVISÓRIA Nº 843 DO PRESIDENTE DA REPÚBLICA, de 5 de julho de 2018, que estabelece requisitos obrigatórios para a comercialização de veículos no País, institui o Programa Rota 2030 - Mobilidade e Logística e dispõe sobre o regime tributário de autopeças não produzidas.
DECRETO Nº 9.557 DO PRESIDENTE DA REPÚBLICA, de 8 de novembro de 2018 Regulamenta a Medida Provisória nº 843, de 5 de julho de 2018, que estabelece requisitos obrigatórios para a comercialização de veículos no País, institui o Programa Rota 2030 - Mobilidade e Logística e dispõe sobre o regime tributário de autopeças não produzidas.

[87] Los beneficios del Plan ROTA 2030 se organizan en torno a tres grandes categorías: promoción en investigación, desarrollo e innovación (I+D+i) por medio de un reintegro para las inversiones referentes a nuevas tecnologías o técnicas productivas, promoción de la seguridad activa y pasiva de los vehículos; y promoción del cuidado medio ambiental, por medio de una reducción de impuestos para vehículos alternativos híbridos y eléctricos.

[88] Otro ejemplo presente en esta área geográfica es el trabajo que desarrolla el Centro de Excelencia y Apropiación en Internet de las Cosas de Colombia, una alianza entre universidades, líderes tecnológicos mundiales y empresas ancla nacionales; que presenta como objetivo potenciar el desarrollo económico de este país desde la tecnología y la innovación, buscando resolver las distintas necesidades de los sectores productivos del país, todo esto apalancado en la formación de talento humano especializado en IoT. Este centro es una iniciativa de esta nación impulsada desde el Ministerio de las TIC, con el apoyo de Colciencias, y corresponde a una estrategia que busca posicionar a Colombia como líder regional en TIC, entre sus líneas de trabajo está la automatización logística, incluyendo los medios de transporte y su estandarización.

fragmentaria y poco coordinada por los gobiernos, por lo que no se ha podido garantizar aún una normalización técnica uniforme o armonizada geográficamente, de los vehículos inteligentes en el conjunto de países de la región, a pesar que en su mayoría están conectados por fronteras terrestres.

III.1.7 Organizaciones internacionales

En la actualidad las normas internacionales para sistemas inteligentes de transporte (incluyendo el coche como parte del sistema) son desarrolladas por organismos como la Unión Internacional de Telecomunicaciones (UIT), la Organización Internacional de Normalización (ISO), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y la Sociedad de Ingenieros Automotrices (SAE International)[89].

Las compañías de la industria automovilística y las organizaciones regionales e internacionales de normalización, como la Unión Internacional de Telecomunicaciones, están trabajando en la elaboración de normas técnicas[90] armonizadas, que garanticen diferentes aspectos relacionados principalmente con la conectividad a nivel global de los vehículos inteligentes[91].

El sector de normalización de la UIT se está abriendo a nuevos miembros de la comunidad de los automóviles y de los seguros, así como a segmentos emergentes del mercado de la Internet de las cosas, M2M[92] y IMT[93]-2020 (5G)[94].

---

[89] Estos organismos de estandarización activos en el campo de los sistemas inteligentes de transporte coordinan su trabajo en una plataforma neutral conocida como Colaboración en los Estándares de Comunicación de Sistemas Inteligentes de Transporte (CITS). Esta coordinación apoya la coherencia, conformidad, interoperabilidad y la compatibilidad entre los estándares de los sistemas inteligentes de transporte, un objetivo que crece en importancia a medida que el despliegue de las soluciones relativas a estos se acelera en todo el mundo.

[90] Entre estas normas técnicas de la UIT se encuentran las que definen los criterios de las plataformas de acceso de los vehículos, las pruebas para evaluar el rendimiento de los teléfonos móviles cuando se utilizan para acceder a los sistemas manos libres de los vehículos, para las actualizaciones de software a través de tecnología por aire a vehículos conectados, sobre la seguridad de las comunicaciones V2X (vehículo a todo) y los criterios de comunicación hablada para las llamadas de emergencia desde los vehículos.

[91] Un destacado ejemplo de esta colaboración en el nuevo Reglamento mundial sobre llamadas de emergencia desde el vehículo, "Sistemas de llamadas de emergencia automáticas", que se refiere a una norma sobre la calidad de la voz en la conectividad de los vehículos.

[92] Máquina a Máquina.

[93] Telecomunicaciones Móviles Internacionales.

[94] Incluyendo el aprendizaje automático e inteligencia artificial, el trabajo en estos sectores emergentes está cobrando nuevas proporciones, dado que tanto los innovadores como los gobiernos y otros actores esperan

Las normas técnicas vinculadas a los vehículos inteligentes que han elaborado y elaboran organismos como la UIT, la SAE[95] y la ISO[96] se han convertido en valiosos complementos de los reglamentos formulados por los países u organizaciones intergubernamentales que los agrupen.

La UIT continúa siendo una ferviente defensora del trabajo de la iniciativa de colaboración de las normas de comunicación de los servicios de transporte inteligentes, que fomenta la cooperación en materia de normas, lo cual resulta fundamental para que desemboque en una serie de normas técnicas que regulen los sistemas de transporte inteligentes[97].

Existen normas técnicas[98] que se aplican a casi todos los niveles de automatización de los vehículos como la ISO 26262 y la SAE J3016; sin embargo existen otros estándares que no abordan completamente las necesidades para los vehículos automatizados y muchos se han desarrollado para dominios o áreas relevantes para la automatización, pero conteniendo lagunas técnicas; algunos de los estándares son desarrollados para apoyar la integración interoperable, otros se centran en describir terminología, capacidades de rendimiento requeridas e interfaces entre subsistemas dentro de los sistemas automatizados[99].

---

que a través de la plataforma de consenso que ha venido a conformar la UIT se faciliten principalmente la conectividad global V2X (vehículo a todo) y las comunicaciones de emergencia desde el vehículo.

[95] Estándar o norma técnica **SAE J3016 "Taxonomía y definiciones de los términos relacionados con los sistemas de automatización de la conducción para vehículos de motor en carretera".**

[96] **ISO 26262 (Automóviles – Seguridad funcional)** es una norma ISO para los sistemas de seguridad en los automóviles. La ISO 26262 define un marco y un modelo de aplicación, así como las actividades, los métodos y los resultados.

[97] ZHAO, HOULIN; LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN; FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.

[98] Como ha podido apreciarse las necesidades relacionadas con el proceso de normalización técnica asociado con la automatización de vehículos se encuentran en varias etapas de identificación, desarrollo, definición y adopción. Los documentos relacionados con la normalización técnica se encuentran aún muy dispersos e incluyen, tanto las normas técnicas de aceptación voluntaria publicadas por las organizaciones de normalización, como por especificaciones descriptivas de acciones a realizar, buenas prácticas y otros tipos de los documentos.

[99] U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

Desde septiembre de 2016[100] se ha creado un grupo conocido como ISO/TC 22/SC 32 que se encuentra desarrollando el estándar único de ciberseguridad ISO 21434[101], que se pueda aplicar al mundo del automóvil y reducir el riesgo de un posible ataque, con intención que entre en vigor a finales de 2019 o durante 2020. Estos esfuerzos incluyen tanto los estándares específicos de automatización y estándares específicos de dominio, por ejemplo: estándares de las tecnologías de la información y la comunicación (TIC) aplicable a subsistemas y tecnologías que luego se integran en el sistema general de automatización o sistema de transporte inteligente; existen también conjuntos de mejores prácticas publicadas y marcos que complementan y se utilizan en conjunto con las normas técnicas voluntarias[102].

III.2 La intervención de los gobiernos en la adopción de políticas y la reglamentación de los vehículos inteligentes

III.2.1 Aspectos generales

La convergencia tecnológica, de normalización técnica y de servicios que implica tanto la confluencia de los fenómenos o de la robótica e inteligencia artificial, el Internet de las Cosas, la 5G y otros medios de conectividad; como que se produzca una convergencia política y normativa cuando se aborde o enfoque la temática de los vehículos inteligentes.

III.2.2 Unión Europea y España

Es por eso que debe valorarse que la Unión Europea además de la normativa que específicamente incide en los vehículos inteligentes, *Directiva (UE) 2010/40 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*

[100] JUEZ, G., [sin fecha]. En 2020, los coches seguirán este estándar de ciberseguridad - HackerCar. *2018* [en línea]. [Consulta: 23 mayo 2019]. Disponible en: https://hackercar.com/estandar-ciberseguridad-automovil/.

[101] Tomado del sitio oficial de referencia sobre el desarrollo de este estándar https://www.iso.org/standard/70918.html

[102] GSMA, 2018. Manual de Políticas Públicas de Telecomunicaciones Móviles 2019. Una guía de temas clave. [en línea]. S.l.: GSMA. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

por carretera y para las interfaces con otros modos de transporte, ha aprobado diferentes normativas[103] para tener en cuenta[104].

En el caso de la Unión Europea, el tráfico rodado es una de las áreas posiblemente más reguladas, dado que se tiene plena conciencia de que conlleva grandes riesgos para todos los usuarios del sistema vial. En este contexto, la automatización de los vehículos cambia los riesgos de conducción en muchos aspectos, lo que requiere una reevaluación de todo el sistema de tráfico y la regulación relacionada con el vehículo. Teniendo en cuenta que las jurisdicciones nacionales pueden obstaculizar el desarrollo de tecnologías para los sistemas o vehículos, la Unión Europea, a través de la UNECE, ha intervenido con el fin de armonizar estas nuevas tecnologías, dado que los enfoques fragmentados de los distintos países dificultarían la aplicación de dichas tecnologías y pondría en peligro la competitividad europea[105].

A tenor de la referida Directiva 2010/40/UE, del Parlamento Europeo y del Consejo, de 7 de julio, al objeto de incorporar al ordenamiento interno español y establecer ese marco general normativo; a través del Real Decreto 662/2012, de 13 de abril, fue establecido el marco general normativo para la implantación de los sistemas inteligentes de transporte (SIT) en el sector del transporte por carretera y para las interfaces con otros modos de transporte, y el uso coordinado y coherente de estos sistemas en España.

---

[103] **Resoluciones del Parlamento Europeo**; de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos; de 13 de marzo de 2018, sobre una estrategia europea sobre los sistemas de transporte inteligentes cooperativos; de 1 de junio de 2017, sobre la conectividad a internet para el crecimiento, la competitividad y la cohesión: la sociedad europea del gigabit y 5G; y de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. **Comunicaciones de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones**; de 7 de diciembre de 2018, Plan coordinado sobre la inteligencia artificial; de 17 de mayo de 2018, En ruta hacia la movilidad automatizada: estrategia de la UE para la movilidad del futuro; y de 13 de noviembre de 2016, Estrategia europea sobre los sistemas de transporte inteligentes cooperativos, un hito hacia la movilidad cooperativa, conectada y automatizada.

[104] Especialmente debe valorarse la Resolución del Parlamento Europeo, de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos; en esta se fijan 23 principios generales a los transportes, 20 específicos a los transportes por carretera; así como otros postulados en materia de derechos de los consumidores, condiciones de competencia y necesidades de formación e investigación, que en todos los casos son aplicables al caso de los vehículos inteligentes.

[105] MONTORO GONZÁLEZ ANA MARTÍ-BELDA BERTOLÍN IGNACIO LIJARCIO PATRICIA BOSÓ CONSUELO LÓPEZ, L. y VILADRICH CASTELLANAS JOSÉ SUÁREZ REYES, R., 2016. *Coche Autónomo, seguridad vial y formación de conductores.* [en línea]. Valencia: [Consulta: 2 mayo 2019]. Disponible en: https://www.cnae.com/ficheros/files/noticias/INFORME Coche autónomo seguridad vial y formación de conductores_ INTRAS-CNAE.pdf.

Entre los aspectos a resaltar de este real decreto es que mediante él se fija las condiciones generales necesarias para alcanzar el objetivo anteriormente referido; y establecer que la aplicación en España de las especificaciones y normas dictadas por la Comisión Europea sobre la implantación de sistemas inteligentes de transporte, debe realizarse conforme a las medidas que, a tal efecto, se adopten por el Ministerio del Interior y el Ministerio de Fomento, en el ámbito de las materias de sus respectivas competencias y respecto a los ámbitos y acciones prioritarios que en este se refieren[106].

III.2.3 Estados Unidos de América

En el caso de EUA, la regulación legislativa referente al desarrollo de la conducción autónoma ha ido avanzando paulatinamente. Los vehículos autónomos se han estado probando por las carreteras estadounidenses desde 2010, cuando Google empezó a probar sus primeros prototipos. Desde entonces, en ausencia de una intervención del Congreso, los estados han estado regulando de manera independiente las normas de uso del vehículo autónomo, creando un mosaico de al menos 21 leyes y pautas estatales distintas[107], con diferentes propósitos y prioridades[108].

California ha sido el estado más permisivo y precoz en cuanto a la regulación de la conducción autónoma, debido principalmente a que allí se encuentra uno de los nichos tecnológicos más importantes del mundo, Silicon Valley. Las normas han variado mucho de un lugar a otro, aunque compartían prácticamente las mismas directrices y principios básicos: *se requiere que haya una persona capacitada ocupando el asiento del conductor. Así mismo, esta persona debe ser capaz de tomar el control absoluto del vehículo en cualquier momento.* A estos principios algunos estados añadían la prohibición de la

[106] Adicionalmente mediante este real decreto se dispone que los sistemas inteligentes de transporte para los que la Comisión Europea no haya adoptado especificaciones o normas se pueden implantar en España de acuerdo con las condiciones y procedimientos técnicos que se determinen por el Ministerio del Interior y el Ministerio de Fomento, en el ámbito de las materias de sus respectivas competencias. Las medidas o disposiciones que se adopten deben estar acorde a 12 principios básicos.

[107] Desde el año 2011, al menos 41 estados en este país de sistema federal han introducido legislación para regular el uso de los vehículos autónomos en carreteras públicas. En 2017, 33 estados aprobaron una nueva normativa o bien actualizaron la existente para favorecer y acelerar su desarrollo tecnológico.

[108] MONTORO GONZÁLEZ ANA MARTÍ-BELDA BERTOLÍN IGNACIO LIJARCIO PATRICIA BOSÓ CONSUELO LÓPEZ, L. y VILADRICH CASTELLANAS JOSÉ SUÁREZ REYES, R., 2016. *Coche Autónomo, seguridad vial y formación de conductores.* [en línea]. Valencia: [Consulta: 2 mayo 2019]. Disponible en: https://www.cnae.com/ficheros/files/noticias/INFORME Coche autónomo seguridad vial y formación de conductores_ INTRAS-CNAE.pdf.

conducción de coches autónomos en vías públicas por ningún otro propósito que no fuera el de testeo o pruebas experimentales[109].

Pero este escenario no es el más deseado por la industria automovilística, que aspira a construir automóviles que puedan circular por todas las vías públicas. El gobierno de EUA reconoce esta situación, y desea encontrar un equilibrio entre permitir que las compañías tecnológicas y de automóviles prueben sus vehículos, dándoles suficiente margen para probar los avances y recopilar datos suficientes y a su vez determinar la mejor manera de llevar a la realidad una conducción autónoma segura[110].

En este contexto, EUA en su afán por liderar la normalización de la conducción autónoma y para evitar perder una "ventaja innovadora" contra China, Rusia, Singapur o Alemania[111], está todavía en proceso de aprobar la primera ley nacional sobre conducción autónoma que permitirá en un futuro fabricar y comercializar vehículos autónomos en todo el país, este proyecto de disposición normativa es conocida como: “American Vision for Safer Transportation through Advancement of Revolutionary Technologies Act’’ or the ‘‘AV START Act”.

El Departamento de Transporte de los EUA ha expresado por su parte que cuando sea necesaria una regulación de los vehículos automatizados y autónomos, buscará establecer reglas que no sean tan prescriptivas y basadas cuando sea posible en el rendimiento; y como punto de partida y hacia el futuro, interpretará y, de acuerdo con todos los requisitos aplicables de notificación y comentarios, adaptará las definiciones de "conductor" y "operador" para reconocer que dichos términos no se refieren exclusivamente a un ser humano, sino que pueden incluir un sistema automatizado[112].

---

[109] MONTORO GONZÁLEZ ANA MARTÍ-BELDA BERTOLÍN IGNACIO LIJARCIO PATRICIA BOSÓ CONSUELO LÓPEZ, L. y VILADRICH CASTELLANAS JOSÉ SUÁREZ REYES, R., 2016. *Coche Autónomo, seguridad vial y formación de conductores.* [en línea]. Valencia: [Consulta: 2 mayo 2019]. Disponible en: https://www.cnae.com/ficheros/files/noticias/INFORME Coche autónomo seguridad vial y formación de conductores_ INTRAS-CNAE.pdf.

[110] Ídem.

[111] TEALE, C., 2018. Federal AV legislation to go no further in Congress. [en línea]. [Consulta: 2 mayo 2019]. Disponible en: https://www.smartcitiesdive.com/news/AV-START-Act-autonomous-vehicle-legislation/544907/.

[112] U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

El Departamento de Transporte de los EUA ha señalado igualmente su visión de fomentar un entorno regulatorio y operativo consistente; apreciando que el conflicto entre las leyes y regulaciones estatales y locales que rodean a los vehículos automatizados crean confusión, introducen barreras y presentan desafíos para su implementación[113].

El Departamento de Transporte de los EUA[114] proporcionará orientación, mejores prácticas, programas piloto y otra asistencia para ayudar a planificar y hacer posible las inversiones necesarias para un futuro automatizado dinámico y flexible en el país; igualmente también se preparará para tecnologías complementarias que mejoran los beneficios de la automatización, como las comunicaciones entre vehículos y el entorno circundante; pero sin asumir la implementación universal, de cualquier enfoque particular.

No obstante lo anterior, el propio sector industrial automovilístico del país junto con otros actores, reconocen que es demasiado pronto para exigir normas dispositivas estrictas y concretas sobre la conducción autónoma, dado que las empresas todavía no están vendiendo estos vehículos al público de forma masiva, tienen que solucionar muchos problemas tecnológicos y todavía están en un proceso de estudio para determinar cómo deben funcionar de manera extensiva y global[115].

III.2.4 China

Coincidentemente con la aprobación de las Directrices finales para el establecimiento del Sistema Nacional de Estándares de la Industria Telemática (Vehículos Inteligentes y

[113] U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

[114] Este ha expresado también que promoverá la consistencia normativa para que los vehículos automatizados puedan funcionar sin problemas en toda la nación; creando consenso entre las agencias de transporte, estatales y locales y las partes de la industria interesadas en estos temas de generación de políticas y normas jurídicas avanzadas, para respaldar la integración de vehículos automatizados en todo el sistema de transporte.

[115] MONTORO GONZÁLEZ ANA MARTÍ-BELDA BERTOLÍN IGNACIO LIJARCIO PATRICIA BOSÓ CONSUELO LÓPEZ, L. y VILADRICH CASTELLANAS JOSÉ SUÁREZ REYES, R., 2016. Coche Autónomo, seguridad vial y formación de conductores. [en línea]. Valencia: [Consulta: 2 mayo 2019]. Disponible en: https://www.cnae.com/ficheros/files/noticias/INFORME Coche autónomo seguridad vial y formación de conductores_ INTRAS-CNAE.pdf.

Conectados); el 26 de diciembre de 2017[116], la Comisión Nacional de Desarrollo y Reforma de China (NDRC) publicó un Plan de Acción de tres años para mejorar la competitividad de la industria manufacturera (2018-2020), una de las acciones claves que incluye este documento es un Plan de Implementación para la Comercialización de Tecnología Clave para Vehículos Inteligentes ("Plan de Implementación")[117].

A partir de la opinión de especialistas del sistema económico y político-normativo chino tanto las Directrices finales y el Plan de implementación son una fuerte evidencia de los esfuerzos del gobierno para ser un líder en la carrera para desarrollar vehículos autónomos[118].

III.2.5 Rusia

Al ser Rusia uno de los pocos países del mundo, que posee un desarrollo endógeno de gran parte del conjunto de tecnologías necesarias para la implementación y operación de vehículos no tripulados: inteligencia artificial, tecnologías de navegación, tecnologías de visión técnica y tecnologías asociadas con el uso de radares lidars; es comprensible que su gobierno haya dispuesto el referido *Reglamento Nº 1415, de 26 de noviembre de 2018, sobre la realización de un experimento para probar el uso de vehículos altamente*

[116] Con anterioridad en julio de 2017, el Consejo de Estado de China emitió el "Plan de Desarrollo de Inteligencia Artificial de Nueva Generación", que describe un ambicioso plan de trabajo para que el país lidere el sector de la inteligencia artificial, priorizando el desarrollo de los vehículos autónomos como una "frontera estratégica". Cinco meses después, el Ministerio de Industria y Tecnología de la Información (MIIT) mejora la hoja de ruta al anunciar el Plan trienal para promover el desarrollo de una industria de inteligencia artificial de nueva generación (2018-2020). El plan de acción incluye planes para desarrollar componentes tecnológicos clave de los vehículos autónomos, como los chips inteligentes para automóviles, los algoritmos de inteligencia del vehículo y los sistemas avanzados de asistencia al conductor.

[117] El objetivo del Plan de Implementación es el establecimiento y operación para 2020 de una plataforma nacional de innovación y un sistema industrial para vehículos inteligentes. Además, pretende mejorar gradualmente la capacidad tecnológica fundamental y lograr más avances en lo que respecta a los sistemas de hardware y software básicos para vehículos inteligentes.

[118] SCHAUB, M. y ZHAO, A., 2018. China Issues Final Guidelines on Standards Establishment for Self-driving Cars. *King & Wood Mallesons Law Firm Web* [en línea]. [Consulta: 11 junio 2019]. Disponible en: https://www.kwm.com/en/knowledge/insights/final-guidelines-on-standards-for-self-driving-cars-20180109#id-here.

automatizados en vías públicas[119], pues sin un ambiente de prueba en la vida real de estas tecnologías no obtendrían experiencia en operaciones reales en entornos urbanos[120].

La posición del gobierno ruso demuestra su objetivo de proporcionar todas las definiciones necesarias para que se desarrolle este transporte, incluida: la definición de qué es un sistema de conducción automatizado, qué o quién posee un vehículo altamente automatizado, implicaciones y consecuencias legales de asumir la responsabilidad por los posibles daños que puedan ser causados por los vehículos inteligentes.

III.2.6 Latinoamérica y el Caribe

Esta área geográfica en su presente no se ha encontrado muchos ejemplos de políticas públicas o reglamentaciones dirigidas a los vehículos inteligentes; aunque se ha reflexionado y analizado sobre el contenido mínimo que se estima deben contener las políticas públicas orientadas al desarrollo del IoT[121] en esta región; contribuyendo tanto con elementos de análisis técnicos y económicos, como a su diseño, ejecución y evaluación; de forma que pueda actuar como palanca para el crecimiento y desarrollo de otros sectores económicos.

A partir de que los vehículos inteligentes constituyen una especie dentro del género del IoT, por analogía se puede tener una idea de la situación que viven los diferentes países respecto a la capacidad de adopción de los vehículos inteligentes, incluida la política y reglamentaria. Un análisis que se ha llevado a cabo teniendo en cuenta un índice basado

[119] Con anterioridad la Orden del Gobierno N ° 535-p del 29 de marzo de 2018 aprobó un plan de acción ("hoja de ruta") para mejorar la legislación y eliminar las barreras administrativas con el fin de garantizar la implementación de la Iniciativa Tecnológica Nacional en el área de Avtonet. Este plan tiene como objetivo garantizar las posiciones prioritarias de las empresas rusas en los mercados globales emergentes, incluido el desarrollo y promoción de productos y servicios en el campo de la logística multimodal, incluida la creación y el desarrollo de plataformas telemáticas de servicio, plataformas de "colaboración para compartir" y otras soluciones de plataforma destinadas a coches conectados ".

[120] De tenerse en cuenta que después de pasar un par de años probando su sistema de conducción autónoma en Moscú y en otras partes de Rusia, Yandex, el equivalente ruso de Google presentó su producto de auto conducción en CES en enero de 2019; esta empresa tiene el objetivo de crear y gestionar una flota de vehículos autónomos, como el Waymo de Alphabet, considerado por muchos como el líder mundial en la carrera por hacer realidad los autos autónomos. Yandex lanzó un servicio de robotaxi en dos ciudades rusas en 2018, aún con un ingeniero detrás del volante.

[121] DELOITTE, 2018. IoT para el Sector Empresarial en América Latina. En: DELOITTE (ed.) [en línea]. Uruguay: Centro de Estudios de Telecomunicaciones de América Latina. [Consulta: 16 marzo 2019]. Disponible en: https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/.

en seis indicadores estrechamente ligados a este ecosistema, capaces de reflejar todos los aspectos y factores relevantes que podrían llegar a afectar al desarrollo de soluciones vinculadas a IoT.

Los resultados arrojados por el índice permiten identificar la realidad que vive la región, al tiempo que se establece una comparación con países más desarrollados. Ambos hechos facilitan la identificación de las barreras que se oponen al desarrollo, así como la forma idónea para reducir la brecha existente con aquellos países más desarrollados[122]. Los indicadores relativos al marco regulatorio y a la situación política económica se relacionan a la capacidad política y reglamentaria, de adopción de los vehículos inteligentes por parte de las naciones latinoamericanas y caribeñas.

III.3 La gestión pública en la salvaguarda de la ciberseguridad de los vehículos inteligentes

III.3.1 Aspectos generales

En la industria del automóvil se está produciendo una clara transición del hardware al software: los vehículos modernos utilizan ahora entre 100 y 150 millones de líneas de código. Esta transición; a la que se suma la convergencia reciente y cada vez más común e inherente de varias tecnologías de avanzada, tanto las generadas propiamente por su industria como por otras, así como la conectividad creciente de los vehículos crea una "tormenta perfecta de problemas de ciberseguridad"[123]. A través de la conectividad, las entidades o personas malintencionadas pueden acceder a la electrónica que controla el arranque del motor, la aceleración, la dirección y los frenos. Los ciberataques pueden poner vidas en peligro, hacer desaparecer la confianza en las tecnologías emergentes y propinar duros golpes a la reputación de las marcas de los fabricantes[124].

[122] DELOITTE, 2018. IoT para el Sector Empresarial en América Latina. En: DELOITTE (ed.) [en línea]. Uruguay: Centro de Estudios de Telecomunicaciones de América Latina. [Consulta: 16 marzo 2019]. Disponible en: https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/.
[123] Explicó Giuseppe Faranda, asesor en materia de ciberseguridad de Karamba Security, durante su participación el 8 de marzo de 2018 en el Simposio sobre los vehículos conectados del futuro (FNC-18), reunión anual organizada por la UIT y la UNECE en el marco del Salón del Automóvil de Ginebra.
[124] Ídem.

Un automóvil inteligente por sus características es considerado como un sistema de control industrial, poseen cada vez en mayor cantidad partes o secciones de automatización y gran parte de sus funcionalidades está centralizada en un controlador de abordo que hace las funciones de Interfaz Hombre-Máquina (HMI por sus siglas en inglés)[125]. Los vehículos inteligentes requieren de extrema atención en temas de seguridad debido a que como se ha referido están compuestos por multitud de sensores[126], cámaras; puertos para la conexión de dispositivos adicionales como unidades de almacenamiento extraíbles, terminales móviles o integrar computadoras personales; y poseen sistemas para el control electrónico de estabilidad, antibloqueo de ruedas, para el control de la presión de las ruedas, de geolocalización, detección de señales y movimientos.

Debido a esta situación los mecanismos de ciberseguridad no pueden limitarse sólo al vehículo, sino también a la propia red de comunicación extremo a extremo entre los vehículos y la infraestructura de soporte, por lo que los actores principales de la industria del automóvil inteligente desplegamos herramientas y esfuerzos para la seguridad dentro de un vehículo; pueden analizarse algunos de los incidentes, eventos, alertas o noticias sobre la seguridad de los vehículos inteligente más relevantes ocurridos en los últimos años obtenidos del sitio institucional del INCIBE-CERT[127].

A partir de estos incidentes, eventos, alertas o noticias sobre la seguridad de los vehículos inteligentes cabe preguntarse: ¿Es suficiente la intervención pública para garantizar los mecanismos de ciberseguridad que requieren los vehículos inteligentes? ¿Cómo pueden colaborar las numerosas partes interesadas, tanto públicas como privadas, para asegurarse de que se desarrolla todo su potencial, más allá de las fronteras y en condiciones seguras para todas las personas? Estas interrogantes anteriores sirven de motivación para comenzar a perfilar el nivel de participación de los estados, en el propósito de garantizar

[125] ALBERCA JAQUERO, C., 2014. Internet of things (IoT). El lado "Inseguro" de las Cosas. En: Carmen Alberca Jaquero (@CarmenAlberca), Consultora del Área de Governance, Risks & Compliance en ECIX GROUP [en línea]. [Consulta: 16 marzo 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/internet-of-things-ciberseguridad.

[126] Por «sensores» se entienden los detectores de un fenómeno físico cuya salida (tras su conversión en una señal que puede ser interpretada por una unidad de control) es capaz de generar «programas» o de modificar instrucciones programadas o datos numéricos de un «programa». Esto incluye los «sensores» con capacidades de visión de máquina, formación de imágenes de infrarrojo, formación de imágenes por ondas acústicas, sensibilidad táctil, fijación de la posición inercial, medición acústica u óptica de distancias, dinamometría o torsiometría. Los sensores inteligentes utilizan un mayor número de protocolos de red estándar e Internet para facilitar la comunicación.

[127] Ver Anexo No. 5 al presente trabajo.

las necesidades de securización efectiva de los vehículos inteligentes y determinar el nivel en que otros actores inciden en esta labor.

III.3.2 Unión Europea y España

La Agencia de la Unión Europea de Seguridad de las Redes y la Información (ENISA) define los autos inteligentes como: *sistemas que brindan funciones conectadas de valor agregado para mejorar la experiencia de los usuarios de autos o mejorar la seguridad de los coches.* ENISA ha identificado determinadas buenas prácticas que garanticen la seguridad de los autos inteligentes contra las amenazas cibernéticas; enumerando los activos sensibles presentes en este tipo de vehículos, así como las amenazas, los riesgos, los factores de mitigación y las posibles medidas de seguridad a implementarse. Esta agencia europea estableció tres categorías de buenas prácticas: ***políticas y estándares, medidas organizativas y funciones de seguridad***[128].

ENISA estableció que para una efectiva protección de los automóviles inteligentes depende de la protección de todos los sistemas involucrados (servicios en la nube, aplicaciones, componentes de automóviles, herramientas de diagnóstico y mantenimiento, etc.); residiendo principalmente el desafío en la seguridad de los componentes de automóviles y productos de posventa, donde las funciones de seguridad deben implementarse a pesar de varios tipos de limitaciones: por ejemplo, la gran cantidad de interfaces para asegurar puede llevar a problemas de planificación y costos; eventualmente, la larga vida útil de los automóviles puede crear la necesidad de requisitos de seguridad dedicados[129].

Debido a los impactos que los ciberataques pueden tener sobre el sistema de un automóvil inteligente; el riesgo para el conductor, sus pasajeros y otros usuarios de la carretera, hace que sea una cuestión de interés europeo y a nivel nacional para los países miembros. ENISA ha desarrollado *una serie de recomendaciones para fabricantes de autos*

[128] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), 2017. Cyber security and resilience of smart cars. Good practices and recommendations. [en línea]. S.l.: [Consulta: 22 mayo 2019]. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/13d4bf8d-e9de-11e6-ad7c-01aa75ed71a1.
[129] Ídem.

inteligentes, proveedores de posventa y compañías de seguros[130]*; para grupos y asociaciones de la industria*131*; y para grupos industriales y asociaciones y empresas de seguridad*[132].

Por su parte en España el INCIBE ha recomendado[133] que las soluciones de seguridad de los coches inteligentes como parte del universo del Internet de las Cosas deben poseer mecanismos de protección de extremo a extremo y múltiples capas para garantizar la seguridad[134].

Debido a las características de los sistemas inteligentes de transporte, incluyendo los coches de igual índole que lo conforman, estos constituyen hoy y continuarán siéndolo en el futuro tanto una infraestructura estratégica[135] como un servicio esencial[136]. Esto

[130] En estas se propone que los actores de la industria establezcan buenas prácticas que mejoren efectivamente la seguridad de sus productos; que el intercambio de información ayude a desafiar la relevancia de sus mecanismos de seguridad según la información de campo y mejorar sus contactos con terceros, especialmente desde el dominio de seguridad, finalmente definir procesos para aclarar su responsabilidad respectiva en caso de que surjan problemas de seguridad.

[131] En este caso están dirigidas a lograr el consenso sobre normas técnicas de buenas prácticas pensadas como una entrada para un esfuerzo de estandarización, en lugar de ser directamente aplicables a un diseño de automóvil específico, a su vez los detalles de los requisitos de seguridad deben definirse en el contexto de las normas. Adicionalmente se debe definir un esquema de evaluación independiente de terceros debido a que los estándares de seguridad existentes para los sistemas automotrices solo abordan marginalmente la seguridad, por lo que se recomienda definir un esquema de evaluación independiente.

[132] Se sugiere que estas entidades construyan herramientas destinadas a realizar pruebas de seguridad y monitoreo de seguridad para que los actores de la industria puedan mejorar directamente sus habilidades de pruebas de este tipo.

[133] INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A. (INCIBE), ENTIDAD PÚBLICA EMPRESARIAL RED.ES (RED.ES), H.T.C.L. (Huawei), 2017. A Building a Trusted and Managed IoT World. [en línea]. S.l.: [Consulta: 22 mayo 2019]. Disponible en: https://www.huawei.com/minisite/iot/img/building_a_trusted_and_managed_iot_world_en.pdf.

[134] Con ellas se hacen hincapié en la seguridad de dispositivos y sensores de forma que se adopten canales de comunicación cifrada que usen claves compartidas por medio de protocolos de comunicación, para garantizar conexiones seguras entre los puntos terminales y la plataforma de gestión, lo que permite garantizar la seguridad de sensores y dispositivos presentes en los coches inteligentes. Lo anterior debe ir acompañado de una securización de la plataforma de gestión para implementar el arranque seguro y verificar la integridad del software y del firmware de los coches, el estado de fiabilidad de todos los dispositivos se informa a la nube y se visualiza. Finalmente se propone que la plataforma en nube privada de la red de transporte deba brindar capacidades de análisis de seguridad basadas en tecnologías de macrodatos y aprendizaje de máquinas, y obtención de registros, eventos e información de tráfico para analizar anomalías en los dispositivos de IoT, en el comportamiento de los usuarios de los puntos terminales y en el estado de la plataforma en nube, también para que pueda identificar y controlar los riesgos de ataques intrusivos en los puntos terminales y la plataforma en nube.

[135] En la Unión Europea y en España lógicamente, como en la mayoría de los países estudiados el sector del transporte de manera general y sin distinción constituye un sector estratégico, en el supuesto español fue establecido como tal mediante la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[136] En virtud de la Disposición Final Primera del Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información; la Comisión Nacional para la Protección de las Infraestructuras Críticas (Comisión PIC), órgano político de mayor entidad del Sistema de Protección de Infraestructuras Críticas (Sistema PIC) aprobó el 30 de octubre de 2018 una primera lista de servicios

implica que las medidas de ciberseguridad pasarán por la correspondencia con su inclusión en esta posición dentro del esquema nacional de seguridad.

III.3.3 Estados Unidos de América

La Administración Nacional de Seguridad del Tráfico en las Carreteras (NHTSA, por sus siglas en inglés); agencia que forma parte del Departamento de Transporte de los Estados Unidos, promueve un enfoque de varias capas para la ciberseguridad al centrarse en los puntos de entrada de un vehículo, tanto los inalámbricos como los con cables, que podrían ser potencialmente vulnerables a un ciberataque[137].

NHTSA ha trabajado con otras agencias gubernamentales, fabricantes de vehículos, proveedores y el público para que la industria pueda abordar eficazmente los desafíos de la ciberseguridad de los vehículos; abarcando varias aplicaciones de seguridad utilizadas en vehículos actuales, así como las previstas para vehículos futuros que podrían presentar formas más avanzadas de automatización y conectividad[138].

De acuerdo con esta agencia un enfoque completo y sistemático de varias capas para la ciberseguridad de los vehículos reduce la posibilidad de que un ciberataque de un vehículo sea exitoso, y mitiga las posibles consecuencias de una intrusión exitosa[139]. NHTSA alienta la formación de Auto-ISAC, un entorno industrial que enfatiza el conocimiento y la colaboración en la ciberseguridad en toda la industria automotriz.

---

esenciales dentro de los sectores incluidos en el ámbito de aplicación (Energía, Transporte, Salud, Sistema financiero, Agua y TIC), designando además a 132 Operadores Esenciales de los 71 Servicios Esenciales aprobados.

[137] NHTSA, 2018. La Ciberseguridad de los Vehículos. [en línea]. [Consulta: 24 abril 2019]. Disponible en: https://www.nhtsa.gov/es/tecnologia-e-innovacion/la-ciberseguridad-de-los-vehiculos.

[138] Esta labor de la NHTSA ha tenido como objetivo expansionar y compartir la base de conocimientos de la ciberseguridad automotriz para establecer mejor los planes de investigación exhaustivos y desarrollar herramientas habilitantes para la investigación aplicada en esta área, apoyar a la industria automotriz en la implementación de mejores prácticas efectivas basadas en la industria y estándares voluntarios para la ciberseguridad y participar en foros de intercambio de información sobre la ciberseguridad, fomentar el desarrollo de nuevas soluciones de sistemas para la ciberseguridad automotriz, y determinar la viabilidad de desarrollar métodos de evaluación del desempeño para la ciberseguridad automotriz.

[139] La propia agencia ha manifestado que este enfoque debe incluir un proceso de identificación y protección basado en el riesgo priorizando los sistemas de control del vehículo que son críticos para la seguridad, la detección oportuna y la respuesta rápida a posibles incidentes de ciberseguridad de los vehículos en las carreteras del país; arquitecturas, métodos y medidas diseñados como parte de las protecciones de ciberseguridad en capas para facilitar la recuperación rápida de incidentes cuando ocurren, y métodos para el intercambio efectivo de inteligencia e información en toda la industria para facilitar la adopción rápida de las lecciones aprendidas en toda la industria.

III.3.4 China

La más reciente normativa sobre esta esfera establecida en China es la denominada Ley de Seguridad Cibernética (CSL), aprobada el 7 de noviembre de 2016 y que entró en vigor el 1 de junio de 2017. Es la primera regulación integral de seguridad y privacidad del ciberespacio en el país, que impone requisitos de cambios de paradigma, como la localización de datos.

La referida normativa de ciberseguridad de esta nación asiática regula en tan solo 79 artículos, aspectos tan dispares como la ciberseguridad, protección de datos personales, las obligaciones de las empresas y el marco sancionador, cuyo contenido normativo en otros países se encuentran dispersos o distribuidos en normas jurídicas de diferente rango normativos o características[140]. Coincido con esta opinión de un excelente analista del Instituto Español de Estudios Estratégicos, que ha expresado igualmente que la brevedad de la referida normativa se consigue mediante una ambigüedad a la hora de su redacción y que dota a su vez al Gobierno chino de mecanismos para la monitorización o control del flujo de información que circula por su territorio o el proteccionismo que han generado reacciones por parte de organizaciones de defensa de derechos humanos, así como de las multinacionales del sector. Las cuestiones sobre derechos y obligaciones de ciudadanos y empresas se abordan desde una aproximación que centraliza la responsabilidad en el Estado, en línea con el modelo de gobernanza nacional del ciberespacio, que el país promueve internacionalmente, diferente al modelo de cooperación público-privada que se promueven por otros estados.

En relación con el objeto de estudio de la presente investigación, tal como lo hace con otras esferas relacionadas con su actividad, sería la Administración del Ciberespacio de China (CAC), la encargada de supervisar y regular todos los aspectos de la ciberseguridad, relacionados con la conectividad de los vehículos inteligentes y conectados.

[140] RAMÍREZ MORÁN, D., 2017. Ciberseguridad en China. *bie3: Boletín I.E.E.E., ISSN-e 2530-125X, Nº 5 (enero - marzo), 2017, págs. 8-15* [en línea], no. 5, pp. 8-15. [Consulta: 13 junio 2019]. ISSN 2530-125X. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6057663.

III.3.5 Rusia

El 26 de julio de 2017, Rusia adoptó la Ley Federal Nº 187-FZ "Sobre la seguridad de la infraestructura de información crítica de la Federación Rusa". La ley establece los principios básicos para garantizar la seguridad de la infraestructura de información crítica, los poderes relacionados de los organismos estatales rusos, así como los derechos, obligaciones y responsabilidades de las personas que poseen instalaciones con infraestructura de información crítica, proveedores de comunicaciones y sistemas de información interactúan con estas instalaciones[141].

La posición del gobierno ruso[142] está basada en la importancia vital que han dado al igual que muchas potencias internacionales, a los elementos de la infraestructura de información crítica como: los sistemas de información, las redes de telecomunicaciones de las autoridades estatales; los sistemas y redes para la gestión de los procesos tecnológicos que se utilizan en la defensa del estado, la asistencia sanitaria, el transporte, las comunicaciones, las finanzas, la energía; así como a las industrias de combustibles, nuclear, aeroespacial, minería, metalmecánica y química[143].

III.3.6 Latinoamérica y el Caribe

En la Asamblea General de la Organización de Estados Americanos (OEA) en 2004, los Estados miembros aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04), proporcionando así el mandato que permite a la Secretaría del Programa de Seguridad

[141] KHAYRYUZOV, V., 2018. Privacy And Cybersecurity In Russia - Data Protection - Russian Federation. *Mondaq.com* [en línea]. [Consulta: 10 junio 2019]. Disponible en: http://www.mondaq.com/russianfederation/x/750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia.

[142] Manifestada ya anteriormente mediante la **Doctrina de Seguridad de la Información de la Federación Rusa**, aprobada por el Presidente de la Federación Rusa Vladimir Putin, el 9 de septiembre del año 2000 y la Estrategia de Seguridad Cibernética de 2014.

[143] Todas estas industrias se consideran críticas para la economía y deben protegerse contra cualquier amenaza cibernética. La ley requiere la implementación de medidas de protección, asignando la categoría de protección (de acuerdo con los estatutos) y luego registrarse en el Servicio Federal de Control Técnico y de Exportaciones, que está a cargo de la supervisión en este campo.

Cibernética de la Secretaría del Comité Interamericano contra el Terrorismo (CICTE por sus siglas en inglés)[144] trabajar en asuntos de seguridad cibernética.

Entre los principales objetivos de la Secretaría, se encuentran el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (CSIRT) en cada país; crear una red de alerta hemisférica que proporcione formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de estrategias nacionales sobre seguridad cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la ciberseguridad en esta región del planeta.

III.4 El uso de los vehículos inteligentes y el tratamiento de datos personales

III.4.1 Aspectos generales

En una sociedad en la que los vehículos que se utilizan por las personas van en camino a la automatización completa de sus sistemas, a alcanzar el mayor nivel de gestión autónoma de la conducción y a estar conectados por vía inalámbrica en todo momento; características tan avanzadas que permiten el desarrollo de modelos de negocios completamente diferentes, adaptados a las tendencias de las nuevas generaciones de seres humanos que por preferencia o necesidad deben acceder de forma colaborativa a los servicios de movilidad, en detrimento de poseer de forma indisoluble un vehículo. Lo anterior puede hacer a esta actividad social más asequible, segura, eficiente y respetuosa con el medioambiente[145].

Muchos servicios de movilidad inteligente se diseñarán para generar, recopilar o compartir datos, algunos de estos (por ejemplo, los relativos al estado físico-técnico de los vehículos o las condiciones meteorológicas de las rutas por donde circulan), no

[144] La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados Miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio.

[145] A su vez la conducción totalmente autónoma y conectada, libera a las personas para realizar otras actividades mientras se trasladan de un lugar a otro; manteniéndose en contacto en tiempo real con sus diferentes redes sociales privadas o públicas, así como con todos los objetos conectados con que se relaciona.

suponen un impacto en la privacidad de los consumidores[146] y, por lo tanto, no deben ser considerados datos personales[147].

Los datos personales que puedan ser recopilados mediante los vehículos inteligente, tienen el potencial de afectar la intimidad y la privacidad de las personas, estando entonces sometidos a leyes generales sobre la protección de datos personales y la privacidad. Cuando los servicios de conectividad de los vehículos sean proporcionados por los propios fabricantes de la industria automovilística o por operadores, de forma que sean catalogados como proveedores de servicios de comunicaciones móviles, también estarán sometidos a las normas sobre privacidad y seguridad específicas del sector de las telecomunicaciones[148].

III.4.2 Unión Europea y España

El Parlamento Europeo y el Consejo de la Unión Europea, en su Directiva (UE) 2010/40, 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, hace referencia a los datos personales generados durante su utilización[149] y las medidas a adoptar para su adecuado tratamiento[150].

---

[146] No obstante, los servicios de movilidad inteligente destinados a los consumidores implican la generación, distribución y uso de datos personales detallados acerca de ellos; por ejemplo: un vehículo inteligente puede utilizar datos acerca del estado físico o de salud de un conductor profesional para determinar que está en condiciones para realizar esta actividad, almacenar información de geolocalización o facilitar el desarrollo de perfiles basados en sus hábitos de compra de servicios de movilidad colaborativa.

[147] GSMA, 2018. Manual de Políticas Públicas de Telecomunicaciones Móviles 2019. Una guía de temas clave. [en línea]. S.l.: GSMA. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

[148] Ídem.

[149] Específicamente en su considerando 12 se expresa que: "*La implantación y el uso de aplicaciones y servicios de sistemas de transporte inteligente conllevará el tratamiento de datos de carácter personal. Este tratamiento debe llevarse a cabo de conformidad con el Derecho de la Unión, tal y como se establece, en particular, en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995* ***(actualmente derogada por REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)*** *, 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, y en 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. Los principios de limitación de la finalidad y de reducción al máximo de los datos, ente otros, deben aplicarse a las aplicaciones de STI".*

[150] En la propia directiva referida en su considerando 13 se expresa que: "*Debe fomentarse el anonimato como uno de los principios de mejorar la privacidad de las personas. Por lo que se refiere a cuestiones relacionadas con la protección de datos y la privacidad en el ámbito de las aplicaciones y los servicios de*

Los postulados mencionados[151] implican que a los fabricantes de automóviles u otros sujetos que intervengan en el tratamiento de datos personales, generados durante la utilización de los vehículos inteligentes; en cumplimiento del Reglamento General de Protección de Datos, les corresponde entre otros deberes jurídicos presentes en esta disposición normativa de la Unión Europea, garantizar la protección de datos personales y la privacidad de los datos desde el diseño de las aplicaciones, de forma que sean cerradas y sólo se transmitan datos con el previo consentimiento explícito del usuario, que deberá ser previamente informado de forma clara y específica, articulando correctamente el acceso o cesión de datos a terceros y cumpliendo con las obligaciones establecidas para el responsable o el encargado del tratamiento[152].

La más reciente Estrategia Nacional de Ciberseguridad de España[153], en su Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas, que responde al Objetivo III de la propia estrategia, expresa como medida tercera: *"3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la identidad digital"*[154].

*STI, la Comisión, si procede, debe consultar en mayor medida al Supervisor Europeo de Protección de Datos y solicitar el dictamen del Grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales (**actualmente Comité Europeo de Protección de Datos establecido por el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, en sus artículos 68 y siguientes)**, creado en virtud del artículo 29 de la Directiva 95/46/CE".* Ambos fundamentos tienen expresión dispositiva en el artículo 10 de esta directiva, vinculado a normas sobre intimidad, seguridad y reutilización de la información.

[151] En la reciente Resolución del Parlamento Europeo, de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos (2018/2089(INI)), se aprecia igualmente la preocupación por el tratamiento de datos personales que se produce durante el uso de los vehículos inteligentes.

[152] RENTERÍA TAZO, A., 2017. Conectividad del vehículo y seguro: desafíos en la industria del automóvil. [en línea]. Madrid: Gómez-Acebo & Pombo. [Consulta: 28 abril 2019]. Disponible en: www.gomezacebo-pombo.com.

[153] El Consejo de Seguridad Nacional español, en su reunión del día 12 de abril de 2019, aprobó la Estrategia Nacional de Ciberseguridad 2019 y mediante su Orden PCI/487/2019, de 26 de abril, procede a su publicación para general conocimiento en el Boletín Oficial del Estado No. 103, de 30 de abril de 2019.

[154] Por su parte en el Real Decreto 662/2012, de 13 de abril, por el que se establece el marco para la implantación de los sistemas inteligentes de transporte (SIT) en el sector del transporte por carretera y para las interfaces con otros modos de transporte, en su disposición adicional primera, se dispone que: "*El tratamiento de los datos de carácter personal necesarios para el funcionamiento de las aplicaciones y los servicios de los sistemas inteligentes de transporte (SIT) se llevará a cabo conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal **(Derogada hoy por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).** Asimismo, en el funcionamiento de las aplicaciones se garantizará siempre que sea posible, el anonimato del interesado y, en todo caso, que sólo se recogerán los datos que resulten imprescindibles para la prestación de los servicios derivados de las mismas."*

Los diferentes tipos de tratamiento de datos personales que vinculados a los sistemas inteligentes de transporte[155], corresponden con los dispuestos por la Agencia Española de Protección de Datos (AEPD)[156], en la lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.4 del RGPD[157].

III.4.3 Estados Unidos de América

En los EUA han valorado que mientras que las tecnologías avanzadas tienen el potencial para proporcionar una enorme seguridad, conveniencia, y otros beneficios importantes para los consumidores, con frecuencia plantean preocupaciones sobre la privacidad[158] de los datos personales como un impedimento potencial para su despliegue.

El Departamento de Transporte de dicho país ha manifestado que en el caso de los vehículos autónomos, considera seriamente la privacidad del consumidor y las

[155] Existe el riesgo de que se produzca la captura de datos personales tanto de forma intencional según este configurado de esta forma por el sistema de control de las cámaras, sensores u otros dispositivos ubicados en el vehículo que pueden recabar este tipo de información o también inintencionada o inadvertida. Esto puede ocurrir al capturar imágenes o datos biométricos de las personas que han abordado el vehículo o de aquellas que se han cruzado durante el recorrido del coche.

[156] A su vez debido a estos tratamientos de datos personales implicados con los coches inteligentes, se tomen por todos los actores implicados, las medidas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos para los derechos y libertades de las personas, en particular para prevenir cualquier tratamiento no autorizado durante las fases de captación, procesamiento, almacenamiento o transmisión de estos datos, por lo que resulta recomendable que se cumpla lo dispuesto en las siguientes documentaciones publicadas por esta propia agencia:

- Guía sobre el uso de videocámaras para seguridad y otras finalidades.
- Guía práctica para las Evaluaciones de Impacto en la Protección de Datos.
- Guía práctica de análisis de riesgos para el tratamiento de datos personales.
- Orientaciones y garantías en los procedimientos de anonimización de datos.

[157] Este listado fue publicado el 9 de mayo de 2019, contiene 11 criterios basados en los establecidos por el Grupo de Trabajo del Artículo 29 en la guía WP248 “Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD”.

[158] El derecho a la privacidad en los EUA se desarrolla en cuatro acciones civiles reconocidas que pueden ejercerse por su violación debido a la intromisión en la reclusión (esfera privada), la invasión de privacidad por apropiación, the false light privacy (distorsión de la imagen) y por la invasión de la privacidad por intromisión y difusión pública de hechos privados; con estas se puede exigir responsabilidad civil y amparar el tratamiento legal a daños relacionadas con la dignidad, con la publicación y con los derechos de propiedad. Estas cuatro clasificaciones están actualmente incorporadas en el Restatement (Second) of Torts, una compilación oficial que aglutina el estado de las leyes de responsabilidad civil estadounidense y forma el basamento legal sobre la privacidad en muchos de los estados que componen esta nación.

implicaciones de privacidad de sus normas de seguridad y orientación voluntaria; y trabaja en estrecha colaboración con la Comisión Federal de Comercio (FTC), la principal agencia federal encargada de proteger la privacidad e información personal de los consumidores, para apoyar su protección y proporcionar recursos relacionados con su privacidad[159].

En ese sentido el Departamento de Transporte de EUA ha lanzado el programa de *Datos para la Integración Automatizada de Vehículos (DAVI por sus siglas en inglés)* como una iniciativa multimodal para identificar, priorizar, monitorear y, cuando sea necesario, abordar las necesidades de intercambio de datos para la integración de vehículos automatizados en todos los modos de transporte; considerando que el acceso a los datos es un elemento habilitante crítico para la integración segura, eficiente y accesible de los vehículos automatizados en el sistema de transporte, y la falta de acceso a estos podría impedir su integración y retrasar su introducción segura. Esto ha determinado que haya establecido una serie principios que buscan evitar esta situación de falta de acceso a los datos, entre estos se incluyen: promover prácticas proactivas de la seguridad basada en datos, ciberseguridad y protección de la privacidad, actuar como facilitador para inspirar y habilitar intercambios voluntarios de datos, empezar pequeño para demostrar valor, y escalar progresivamente hacia una visión más amplia y coordinar a través de mecanismos para la reducir de los costos, reducir la carga de la industria y acelerar las acciones[160].

III.4.4 China

Como ha sido mencionado en el caso chino la denominada Ley de Seguridad Cibernética, regula junto con otros aspectos tanto la ciberseguridad como la protección de datos

[159] U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

[160] A partir de la visión del Departamento de Transporte de EUA la industria en su conjunto debería considerar trabajar con agencias federales, estatales y locales así como con los organismos de normalización técnica pertinentes (IEEE, SAE Internacional, etc.) para identificar oportunidades de establecer intercambios voluntarios de datos que puedan proporcionar beneficio mutuo y ayudar a acelerar la integración segura de la automatización en el sistema de transporte de superficie. Esto puede incluir intercambios de datos entre el sector público y el privado en cuanto a condiciones de infraestructura, así como los intercambios entre las entidades del sector privado que permita el aprendizaje mutuo y la mitigación del riesgo en cuanto a los datos personales.

personales, aplicándose a “operadores de red”[161] y operadores de “infraestructuras críticas de información”[162], aunque estos últimos están sujetos a requisitos más estrictos.

La "información personal" y los "datos importantes" recopilados o generados por estos operadores en China deben almacenarse en el país, esto queda recogido en el Art. 37 de la ley[163], de lo cual un claro caso para su aplicación sería los datos recopilados mediante los vehículos inteligentes y conectados. La propia ley prevé que cuando un operador necesite transferir dichos datos al extranjero, debe demostrar la necesidad de exportar los datos y realizar una evaluación de seguridad personal o enviarla a una evaluación de seguridad oficial cuando se cumple una prueba de umbral[164].

Además de la localización de datos y las evaluaciones de seguridad, los operadores de red de vehículos inteligentes y autónomos en China deben cumplir con otras medidas relacionadas con la ciberseguridad y la protección de datos personales incluidas en los artículos 21, 41 al 43, 46-47 y 49 de la citada disposición normativa[165].

III.4.5 Rusia

La Ley Federal No. 152-FZ sobre Datos Personales de fecha 27 de julio de 2006 (la Ley de PD) es la ley principal que rige la información de identificación personal (datos personales) en Rusia y seria la normativa aplicable en caso del tratamiento de datos personales vinculados a los vehículos inteligentes. Esta ley rusa se adoptó en 2005 tras la ratificación del Convenio del Consejo de Europa para la protección de las personas con respecto al procesamiento automático de datos personales y se basa en los instrumentos

[161] Este término tal como ha sido definido en esta normativa pude incluir "propietarios, operadores y proveedores de servicios de redes", es decir a cualquier compañía que ofrezca servicios o negocios operativos a través de una red de computadoras.
[162] El alcance de este término abarca a las empresas de sectores críticos como la radio, la televisión, la energía, el transporte, la conservación del agua, las finanzas y el servicio público, u otra infraestructura de información crítica cuya afectación, destrucción, pérdida de funcionalidad o fuga de datos pueda causar graves daños a la seguridad del estado, a la economía nacional, al sustento del pueblo chino y al interés público.
[163] RAMÍREZ MORÁN, D., 2017. Ciberseguridad en China. *bie3: Boletín I.E.E.E., ISSN-e 2530-125X, Nº 5 (enero - marzo), 2017, págs. 8-15* [en línea], no. 5, pp. 8-15. [Consulta: 13 junio 2019]. ISSN 2530-125X. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6057663.
[164] CHIN, M., LIU, C. y ZHANG, X., 2018. China’s Cybersecurity Law. *Reed Smith LLP Web* [en línea]. S.l.: [Consulta: 13 junio 2019]. Disponible en: https://www.reedsmith.com/en/perspectives/2018/01/chinas-cybersecurity-law.
[165] Ídem.

internacionales sobre privacidad y protección de datos en ciertos aspectos, pero la regulación rusa hace especial hincapié en las medidas técnicas para la protección de datos. Las disposiciones de protección de datos también se pueden encontrar en otras leyes sectoriales, incluida la Ley Federal Nº 149-FZ en Información, Tecnologías de la Información y protección de la información del 2006 y el capítulo 14 del Código del Trabajo de la Federación de Rusia de 2001[166].

Además, numerosos requisitos legales y técnicos se establecen en los reglamentos emitidos por las autoridades gubernamentales rusas en el ámbito de la protección de datos, a saber; el Servicio Federal de Comunicaciones, Tecnología de la Información y Supervisión de Comunicaciones en Masa (conocido como Roskomnadzor), el Servicio Federal para el Control Técnico y de Exportación (FSTEK) y el Servicio de Seguridad Federal (FSS). Las regulaciones en esta área son constantemente enmendadas y desarrolladas[167].

III.4.6 Latinoamérica y el Caribe

América Latina presenta una situación totalmente diferente a la vista en la Unión Europea o EUA en cuanto la protección de datos personales y que impacta en su relación con los vehículos inteligentes; cada país ha abordado la protección de datos y privacidad de una forma diferente[168], aunque es necesario destacar el impacto de la regulación europea en el escenario latinoamericano.

El marco legal de las naciones latinoamericanas sobre protección de datos personales[169] ha sufrido modificaciones en los últimos años; en Argentina, Chile, Colombia, Brasil, Ecuador, México, Perú y Uruguay se han promulgado desde 2008 leyes específicas sobre esta temática; Paraguay tiene varias normativas que abarcan de forma dispersa y no específica el tratamiento de datos personales: recolección, uso y autoridad de aplicación

[166]LAW FIRM GORODISSKY & PARTNERS, 2017. Data protection in Russian Federation: overview. *Gorodissk.com* [en línea]. [Consulta: 10 junio 2019]. Disponible en: http://www.gorodissky.com/publications/articles/data-protection-in-russian-federation-overview/.
[167] Ídem.
[168] Ver para más detalle la Gráfico I.- Situación regulatoria de la protección de los datos personales en Latinoamérica, anexa al presente trabajo.
[169] DELOITTE, 2018. IoT para el Sector Empresarial en América Latina. En: DELOITTE (ed.) [en línea]. Uruguay: Centro de Estudios de Telecomunicaciones de América Latina. [Consulta: 16 marzo 2019]. Disponible en: https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/.

para cada caso; Venezuela sigue brindando protección con leyes sectoriales; otros como Cuba, recientemente han normado de manera general y por primera vez esta temática en su nueva Constitución[170], aprobada por su parlamento en diciembre de 2018 y posteriormente ratificada en un referéndum popular celebrado el 24 de febrero de 2019.

El obligatorio cumplimiento del Reglamento General de Protección de Datos (RGPD) a partir de mayo de 2018, ha tenido un impacto en todas las regiones del mundo, debido a que establece que todas las empresas del mundo que cuenten con datos de clientes europeos deben acogerse a su cumplimiento. Este factor puede ayudar a la homogeneización y armonización de las normas de privacidad y puede suponer un impulso global para la adopción de un modelo similar al europeo y que por supuesto impactará en todo lo relacionado a los vehículos inteligentes.

[170] La nueva ley de leyes cubana de 2019 expresa en su texto que: *ARTÍCULO 97. Se reconoce el derecho de toda persona de acceder a sus datos personales en registros, archivos u otras bases de datos e información de carácter público, así como a interesar su no divulgación y obtener su debida corrección, rectificación, modificación, actualización o cancelación. El uso y tratamiento de estos datos se realiza de conformidad con lo establecido en la ley.*

Conclusiones y Recomendaciones

A partir del desarrollo de este estudio se pueden presentar las conclusiones y recomendaciones siguientes:

Conclusiones:

Primera: Aunque desde su nacimiento, el sector automovilístico ha sido líder en la investigación e innovación, cuando se le comparaba con otras actividades industriales; en el presente, su devenir está sujeto al actuar de otros actores no tradicionales, que se han convertido en sus impulsores actuales; estimando que su tendencia de desarrollo estará marcada por los vehículos inteligentes, alimentados por fuentes renovables de energía, autónomos, conectados y de uso compartido.

Segunda: Cuando se aborde o enfoque la temática de los vehículos inteligentes, debe tenerse en cuenta principalmente, que estos impactan sobremanera, tanto en la convergencia tecnológica de normalización técnica, ciberseguridad y de servicios, así como, en la confluencia de los fenómenos o de la robótica e inteligencia artificial, el Internet de las Cosas, la 5G y otros medios de conectividad.

Tercera: Debido a que su utilización es global, la normalización técnica o estandarización va a ser esencial para elaborar un ecosistema seguro de vehículos inteligentes, con estándares lo más homogéneo posible en todos los países; que facilite la integración creciente de las tecnologías de la información y las comunicaciones en los vehículos con la seguridad vial, la protección de datos personales y la interoperabilidad, como capacidad de los sistemas y de los procesos empresariales subyacentes, para intercambiar datos y compartir información y conocimientos.

Cuarta: La convergencia de la tecnología del automóvil, las telecomunicaciones y las tecnologías de la información y la comunicación (TIC) han permitido desarrollar, nuevos modelos de negocios en los servicios de conectividad; no obstante, a través de esta nueva conectividad, sujetos malintencionados pueden acceder a la electrónica que controla el arranque del motor, la aceleración, la dirección y los frenos, ciberataques que pueden

poner vidas en peligro, hacer desaparecer la confianza en las tecnologías emergentes y generar daños reputacionales de las marcas de los fabricantes.

Quinta: Si bien han sido implementados proyectos relativos a coches inteligentes, mediante aplicaciones nativas o foráneas de estas tecnologías en el sector del transporte por carretera en diferentes países; sin embargo, aún es insuficiente en muchos casos, el nivel de preparación en términos de avance y capacidad para su introducción.

Sexta: La mayoría de los países no tienen políticas públicas, planes de acción, estrategias o legislaciones que mencionen o regulen específicamente los vehículos inteligentes, por lo que se aplicarían los documentos o instrumentos de este tipo que puedan incidir directa o indirectamente en estos, por convergencia política y normativa.

Séptima: En el presente, las normativas y legislaciones de diferentes naciones, que pretenden plasmar los factores del desarrollo sostenible y seguro de los vehículos inteligentes, para hacerlos operativos, presentan diferencias entre las orientaciones adoptadas en función de los territorios en los que se aplican y sus particularidades; insistiendo en imprimirles particularidades locales o regionales, marcadas por los intereses de cada una de las principales potencias implicadas, conllevando a que dicha implantación se efectúe en ocasiones de forma fragmentaria y poco coordinada por los gobiernos, impidiendo garantizar una continuidad uniforme o armonizada a nivel global.

Recomendaciones

Primera: Dar seguimiento al proceso de normalización técnica e implementación político-jurídica de los vehículos inteligentes en el mundo, con especial énfasis en el derrotero futuro de la ciberseguridad y la protección de datos personales.

Segunda: Evaluar desde el punto de vista de la ciberseguridad y la protección de datos personales, la evolución del proyecto piloto a realizarse hasta el 2022 para toda la ciudad de León, España; en lo relacionado con vehículos autónomos nivel 4 y 5, impulsado por el capítulo español de la Asociación Internacional de Sistemas de Vehículos No Tripulados (AUSI-SPAIN) y con la implicación directa de la compañía de ingeniería y diseño de movilidad "DROTIUM".

Bibliografía

ADOLPH, M., ANDREEV, D., AUBINEAU, P., BEDI, I., BOZSÓKI, I., BUETI, C., BUONOMO, S., HUSENOVIC, K., JAMOUSSI, B., KARYABWITE, D., KURAKOVA, T., MADDENS, S., MANIEWICZ, M., OTA, H., RESTREPO, J., SUNDBERG, N., TOMIMURA, D. y VASSILIEV, N., 2018. Sentando las bases para la 5G: Oportunidades y desafíos. [en línea]. 1ra. Ginebra, Suiza. [Consulta: 13 febrero 2019]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf.

BARATTA MARTÍNEZ, R., 2018. Gobierno de la Ciberseguridad. *Economía industrial, ISSN 0422-2784, Nº 410, 2018 (Ejemplar dedicado a: Ciberseguridad), págs. 61-70* [en línea]. S.l.: Ministerio de Industria y Energía [Secretaria General Técnica del Miner], pp. 61-70. [Consulta: 7 marzo 2019]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6815102.

BOSÓ SEGUÍ, PATRICIA; LIJARCIO CÁRCEL, JOSÉ IGNACIO; LÓPEZ OSMA, CONSUELO; MARTÍ-BELDA BERTOLÍN, ANA; Y MONTORO GONZÁLEZ, L., 2018. Estudio sobre la opinión de los conductores españoles sobre el vehículo autónomo. [en línea]. Valencia, España: [Consulta: 2 mayo 2019]. Disponible en: https://drive.google.com/file/d/1Sw7-fn3QgfdxaeqfRzhjjuWeQ0b2Z7zy/view.

CC.OO., Á.D.E.E.S., 2018. Situación y perspectivas en el sector del automóvil. Medidas ambientales, digitalización y automatización de la industria. [en línea]. Madrid, España: CC.OO Área de Estrategias Sectoriales. [Consulta: 23 enero 2019]. Disponible en: http://www.industria.ccoo.es/30f03016ef175ac370e57b5f43e44267000060.pdf.

CENTRO CRIPTOLÓGICO NACIONAL, 2017. CCN-CERT BP/05 Internet de las Cosas. [en línea]. España: [Consulta: 23 mayo 2019]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2261-ccn-cert-bp-05-internet-de-las-cosas-1/file.html.

CHIN, M., LIU, C. y ZHANG, X., 2018. China's Cybersecurity Law. *Reed Smith LLP Web* [en línea]. S.l.: [Consulta: 13 junio 2019]. Disponible en: https://www.reedsmith.com/en/perspectives/2018/01/chinas-cybersecurity-law.

DELOITTE, 2018. IoT para el Sector Empresarial en América Latina. En: DELOITTE (ed.) [en línea]. Uruguay: Centro de Estudios de Telecomunicaciones de América Latina. [Consulta: 16 marzo 2019]. Disponible en: https://cet.la/estudios/cet-la/iot-

sector-empresarial-america-latina/.

DIVISIÓN DE ESTUDIOS Y TECNOLOGÍA DEL TRANSPORTE DE LA y SECRETARÍA GENERAL DE TRANSPORTE, con la colaboración del equipo técnico de I., 2019. La transformación digital en el transporte. [en línea]. Madrid: [Consulta: 19 mayo 2019]. Disponible en: http://observatoriotransporte.fomento.es/NR/rdonlyres/71203DCA-E2E4-4E33-8C05-1A94DEBAB20A/151260/MONOGRAFICO_DIGITALIZACION_TRANSPORTE.pdf.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), 2017. Cyber security and resilience of smart cars. Good practices and recommendations. [en línea]. S.l.: [Consulta: 22 mayo 2019]. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/13d4bf8d-e9de-11e6-ad7c-01aa75ed71a1.

FOMENTO, M. de, 2012. Estudio de diagnosis de la situación actual de implantación y de demanda de las nuevas tecnologías en el transporte por carretera y ferrocarril. [en línea]. S.l.: [Consulta: 19 mayo 2019]. Disponible en: http://www.fomento.gob.es/MFOM.DGTT.CatalogoElectronico.web/.

GALÍN, A., 2018. Standardization of connectivity technologies for autonomous vehicles: C-V2X, U-V2X and 5G (Part 1). *The Applus+Blog* [en línea]. [Consulta: 11 junio 2019]. Disponible en: http://blog.applus.com/standardization-connectivity-technologies-autonomous-vehicles-c-v2x-u-v2x-5g-part-1/.

GSMA, 2018. Manual de Políticas Públicas de Telecomunicaciones Móviles 2019. Una guía de temas clave. [en línea]. S.l.: GSMA. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

HUQ, N., VOSSELER, R. y SWIMMER, M., 2017. Cyberattacks Against Intelligent Transportation Systems: Assessing Future Threats to ITS. [en línea]. S.l.: [Consulta: 19 mayo 2019]. Disponible en: http://www.computing.es/siteresources/files/839/02.pdf.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A. (INCIBE), ENTIDAD PÚBLICA EMPRESARIAL RED.ES (RED.ES), H.T.C.L. (Huawei), 2017. A Building a Trusted and Managed IoT World. [en línea]. S.l.: [Consulta: 22 mayo

2019]. Disponible en: https://www.huawei.com/minisite/iot/img/building_a_trusted_and_managed_iot_world_en.pdf.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A. (INCIBE), 2018. Tecnologías emergentes, IoT y ciberseguridad. [en línea]. [Consulta: 16 marzo 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/tecnologias-emergentes-iot-y-ciberseguridad.

KOSTER, ALEX; KUHNERT, FELIX; STÜRMER, C., 2017. Five trends transforming the Automotive Industry. [en línea]. S.l.: PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. [Consulta: 25 marzo 2019]. Disponible en: https://www.pwc.at/de/publikationen/branchen-und-wirtschaftsstudien/eascy-five-trends-transforming-the-automotive-industry_2018.pdf.

KPMG INTERNATIONAL, 2019. 2019 Autonomous Vehicles Readiness Index. [en línea]. Ginebra, Suiza: KPMG International. [Consulta: 25 marzo 2019]. 136024-G. Disponible en: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf.

LAW FIRM GORODISSKY & PARTNERS, 2017. Data protection in Russian Federation: overview. *Gorodissk.com* [en línea]. [Consulta: 10 junio 2019]. Disponible en: http://www.gorodissky.com/publications/articles/data-protection-in-russian-federation-overview/.

MIKOLIC-TORREIRA, I., HENRY, R., SNYDER, D., BEAGHLEY, S., PETTYJOHN, S.L., HARTING, S., WESTERMAN, E., SHLAPAK, D.A., BISHOP, M., OBERHOLTZER, J., SKRABALA, L. y WEINBAUM, C., 2016. A Framework for Exploring Cybersecurity Policy Options. [en línea]. S.l.: [Consulta: 19 mayo 2019]. Disponible en: www.rand.org/t/RR1700.

MONTORO GONZÁLEZ ANA MARTÍ-BELDA BERTOLÍN IGNACIO LIJARCIO PATRICIA BOSÓ CONSUELO LÓPEZ, L. y VILADRICH CASTELLANAS JOSÉ SUÁREZ REYES, R., 2016. Coche Autónomo, seguridad vial y formación de conductores. [en línea]. Valencia: [Consulta: 2 mayo 2019]. Disponible en: https://www.cnae.com/ficheros/files/noticias/INFORME Coche autónomo seguridad vial y formación de conductores_ INTRAS-CNAE.pdf.

RAMÍREZ MORÁN, D., 2017. Ciberseguridad en China. *bie3: Boletín I.E.E.E., ISSN-e 2530-125X, Nº 5 (enero - marzo), 2017, págs. 8-15* [en línea], no. 5, pp. 8-15.

[Consulta: 13 junio 2019]. ISSN 2530-125X. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6057663.

RENTERÍA TAZO, A., 2017. Conectividad del vehículo y seguro: desafíos en la industria del automóvil. [en línea]. Madrid: Gómez-Acebo & Pombo. [Consulta: 28 abril 2019]. Disponible en: www.gomezacebo-pombo.com,.

SCHAUB, M. y ZHAO, A., 2018. China Issues Final Guidelines on Standards Establishment for Self-driving Cars. *King & Wood Mallesons Law Firm Web* [en línea]. [Consulta: 11 junio 2019]. Disponible en: https://www.kwm.com/en/knowledge/insights/final-guidelines-on-standards-for-self-driving-cars-20180109#id-here.

U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

UNIÓN INTERNACIONAL, DE TELECOMUNICACIONES (UIT), EL BANCO MUNDIAL, la S. de la C., (COMSEC), LA ORGANIZACIÓN DE TELECOMUNICACIONES DE LA COMMONWEALTH (CTO), E. y CENTRO DE EXCELENCIA DE CIBERDEFENSA COOPERATIVA DE LA OTAN (CCDCOE OTAN), 2018. Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad. [en línea]. S.l.: [Consulta: 10 junio 2019]. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS Guide_s.pdf.

ZHAO, HOULIN; IBARAKI, STEPHEN; SAHOTA, NEIL; NARAIN, NIVEN R.; AKHTMAN, JOSEF; KHALDI, NORA; BROWNE, EMMET; HINCHEY, MIKE; WERNER, FREDERIC; BANIFATEMI, A., 2018. Nuevas fronteras reglamentarias. Cómo las tecnologías emergentes están dando lugar a enormes oportunidades y desafíos potenciales. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 24 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-03/2018_ITUNews03-es.pdf.

ZHAO, HOULIN;LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN;

FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.

ZHAO, H. y VECCHIONE, MAURIZIO;HERWEIJER, CELINE; STEWART, UYI; IBARAKI, STEPHEN; ZURUTUZA, NAROA; SAHOTA, NEIL; FENECH, MATTHEW; SALIBA, T., 2018. Inteligencia artificial para el bien del mundo. *ITU News Magazine* [en línea]. Ginebra: Unión Internacional de Telecomunicaciones. [Consulta: 14 junio 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-01/2018_ITUNews01-es.pdf.

Legislación

Brasil

MEDIDA PROVISÓRIA Nº 843 DO PRESIDENTE DA REPÚBLICA, de 5 de julho de 2018, que estabelece requisitos obrigatórios para a comercialização de veículos no País, institui o Programa Rota 2030 - Mobilidade e Logística e dispõe sobre o regime tributário de autopeças não produzidas.

DECRETO Nº 9.557 DO PRESIDENTE DA REPÚBLICA, de 8 de novembro de 2018 Regulamenta a Medida Provisória nº 843, de 5 de julho de 2018, que estabelece requisitos obrigatórios para a comercialização de veículos no País, institui o Programa Rota 2030 - Mobilidade e Logística e dispõe sobre o regime tributário de autopeças não produzidas.

China

Ley de Seguridad Cibernética (CSL), aprobada el 7 de noviembre de 2016 (Traducción No Oficial al Español).

Cuba

Constitución de la República de Cuba del año 2019.

España

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Real Decreto 662/2012, de 13 de abril, por el que se establece el marco para la implantación de los sistemas inteligentes de transporte (SIT) en el sector del transporte por carretera y para las interfaces con otros modos de transporte.

Instrucción No. 15/V-113 de la Dirección General de Tráfico del Ministerio del Interior, de 13 de noviembre de 2015, sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general.

Instrucción No. 16 TV/89 de la Dirección General de Tráfico del Ministerio del Interior, de 20 de enero de 2016, sobre la autorización del uso de los sistemas de estacionamiento asistido de vehículos a motor para emplearse en las vías abiertas al tráfico.

Organización de las Naciones Unidas

Convención de Viena sobre la Circulación Vial de 1968.

Rusia

Reglamento Nº 1415, de 26 de noviembre de 2018, sobre la realización de un experimento para probar el uso de vehículos altamente automatizados en vías públicas (Traducción No Oficial al Español).

Unión Europea

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

REGLAMENTO (UE) 2019/796 DEL CONSEJO, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros.

DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

DIRECTIVA (UE) 2010/40 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.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 15 de enero de 2019, sobre la conducción autónoma en los transportes europeos (2018/2089(INI)).

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 13 de marzo de 2018, sobre una estrategia europea sobre los sistemas de transporte inteligentes cooperativos (2017/2067(INI)).

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 1 de junio de 2017, sobre la conectividad a internet para el crecimiento, la competitividad y la cohesión: la sociedad europea del gigabit y 5G (2016/2305(INI)).

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, de 7 de diciembre de 2018, Plan coordinado sobre la inteligencia artificial (COM (2018) 795 final).

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, de 17 de mayo de 2018, En ruta hacia la movilidad automatizada: estrategia de la UE para la movilidad del futuro (COM (2018) 283 final).

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, de 13 de noviembre de 2016, Estrategia europea sobre los sistemas de transporte inteligentes cooperativos, un hito hacia la movilidad cooperativa, conectada y automatizada (COM (2016) 766 final).

Estrategias Públicas vinculadas a la Ciberseguridad de los Vehículos Inteligentes

España

Estrategia de Seguridad Nacional 2017 aprobada por el Consejo de Ministros mediante el Real Decreto 1008/2017, de 1 de diciembre, publicada en el Boletín Oficial del Estado No. 309, de 21 de diciembre de 2017.

Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023 aprobada por el Consejo de Seguridad Nacional español, en su reunión del día 21 de enero de 2019, publicada para general conocimiento en el Boletín Oficial del Estado No. 46, de 22 de febrero de 2019, mediante la Orden PCI/161/2019, de 21 de febrero.

Estrategia Nacional contra el Terrorismo 2019 aprobada por el Consejo de Seguridad Nacional español, en su reunión del día 21 de enero de 2019, publicada para general conocimiento en el Boletín Oficial del Estado No. 49, de 26 de febrero de 2019, mediante la Orden PCI/179/2019, de 22 de febrero.

Estrategia Nacional de Ciberseguridad 2019 aprobada por el Consejo de Seguridad Nacional español, en su reunión del día 12 de abril de 2019, publicada para general conocimiento en el Boletín Oficial del Estado No. 103, de 30 de abril de 2019, mediante la Orden PCI/487/2019, de 26 de abril.

Otras fuentes de información

ADOLPH, M., ANDREEV, D., AUBINEAU, P., BEDI, I., BOZSÓKI, I., BUETI, C., BUONOMO, S., HUSENOVIC, K., JAMOUSSI, B., KARYABWITE, D., KURAKOVA, T., MADDENS, S., MANIEWICZ, M., OTA, H., RESTREPO, J., SUNDBERG, N., TOMIMURA, D. y VASSILIEV, N., 2018. Sentando las bases para la 5G: Oportunidades y desafíos. [en línea]. 1ra. Ginebra, Suiza: #s3gt_translate_tooltip_mini { display: none !important; }. [Consulta: 13 febrero 2019]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf.

BARATTA MARTÍNEZ, R., 2018. Gobierno de la Ciberseguridad. *Economía industrial, ISSN 0422-2784, Nº 410, 2018 (Ejemplar dedicado a: Ciberseguridad), págs. 61-70* [en línea]. S.l.: Ministerio de Industria y Energía [Secretaria General Técnica del Miner], pp. 61-70. [Consulta: 7 marzo 2019]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6815102.

BOSÓ SEGUÍ, PATRICIA; LIJARCIO CÁRCEL, JOSÉ IGNACIO; LÓPEZ OSMA, CONSUELO; MARTÍ-BELDA BERTOLÍN, ANA; Y MONTORO GONZÁLEZ, L., 2018. Estudio sobre la opinión de los conductores españoles sobre el vehículo autónomo. [en línea]. Valencia, España: [Consulta: 2 mayo 2019]. Disponible en: https://drive.google.com/file/d/1Sw7-fn3QgfdxaeqfRzhjjuWeQ0b2Z7zy/view.

CC.OO., Á.D.E.E.S., 2018. Situación y perspectivas en el sector del automóvil. Medidas ambientales, digitalización y automatización de la industria. [en línea]. Madrid, España: CC.OO Área de Estrategias Sectoriales. [Consulta: 23 enero 2019]. Disponible en: http://www.industria.ccoo.es/30f03016ef175ac370e57b5f43e44267000060.pdf.

CENTRO CRIPTOLÓGICO NACIONAL, 2017. CCN-CERT BP/05 Internet de las Cosas. [en línea]. España: [Consulta: 23 mayo 2019]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2261-ccn-cert-bp-05-internet-de-las-cosas-1/file.html.

CHIN, M., LIU, C. y ZHANG, X., 2018. China's Cybersecurity Law. *Reed Smith LLP Web* [en línea]. S.l.: [Consulta: 13 junio 2019]. Disponible en: https://www.reedsmith.com/en/perspectives/2018/01/chinas-cybersecurity-law.

DELOITTE, 2018. IoT para el Sector Empresarial en América Latina. En: DELOITTE (ed.) [en línea]. Uruguay: Centro de Estudios de Telecomunicaciones de América

Latina. [Consulta: 16 marzo 2019]. Disponible en: https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/.

DIVISIÓN DE ESTUDIOS Y TECNOLOGÍA DEL TRANSPORTE DE LA y SECRETARÍA GENERAL DE TRANSPORTE, con la colaboración del equipo técnico de I., 2019. La transformación digital en el transporte. [en línea]. Madrid: [Consulta: 19 mayo 2019]. Disponible en: http://observatoriotransporte.fomento.es/NR/rdonlyres/71203DCA-E2E4-4E33-8C05-1A94DEBAB20A/151260/MONOGRAFICO_DIGITALIZACION_TRANSPORTE.pdf.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), 2017. Cyber security and resilience of smart cars. Good practices and recommendations. [en línea]. S.l.: [Consulta: 22 mayo 2019]. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/13d4bf8d-e9de-11e6-ad7c-01aa75ed71a1.

FOMENTO, M. de, 2012. Estudio de diagnosis de la situación actual de implantación y de demanda de las nuevas tecnologías en el transporte por carretera y ferrocarril. [en línea]. S.l.: [Consulta: 19 mayo 2019]. Disponible en: http://www.fomento.gob.es/MFOM.DGTT.CatalogoElectronico.web/.

GALÍN, A., 2018. Standardization of connectivity technologies for autonomous vehicles: C-V2X, U-V2X and 5G (Part 1). *The Applus+Blog* [en línea]. [Consulta: 11 junio 2019]. Disponible en: http://blog.applus.com/standardization-connectivity-technologies-autonomous-vehicles-c-v2x-u-v2x-5g-part-1/.

GSMA, 2018. Manual de Políticas Públicas de Telecomunicaciones Móviles 2019. Una guía de temas clave. [en línea]. S.l.: GSMA. Disponible en: https://www.gsma.com/publicpolicy/mobilepolicyhandbook/wp-content/uploads/2019/01/GSMA_MPH7_linked_pages_ESP.pdf.

HUQ, N., VOSSELER, R. y SWIMMER, M., 2017. Cyberattacks Against Intelligent Transportation Systems: Assessing Future Threats to ITS. [en línea]. S.l.: [Consulta: 19 mayo 2019]. Disponible en: http://www.computing.es/siteresources/files/839/02.pdf.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A. (INCIBE), ENTIDAD PÚBLICA EMPRESARIAL RED.ES (RED.ES), H.T.C.L. (Huawei), 2017. A

Building a Trusted and Managed IoT World. [en línea]. S.l.: [Consulta: 22 mayo 2019]. Disponible en: https://www.huawei.com/minisite/iot/img/building_a_trusted_and_managed_iot_world_en.pdf.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, S.A. (INCIBE), 2018. Tecnologías emergentes, IoT y ciberseguridad. [en línea]. [Consulta: 16 marzo 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/tecnologias-emergentes-iot-y-ciberseguridad.

KOSTER, ALEX; KUHNERT, FELIX; STÜRMER, C., 2017. Five trends transforming the Automotive Industry. [en línea]. S.l.: PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. [Consulta: 25 marzo 2019]. Disponible en: https://www.pwc.at/de/publikationen/branchen-und-wirtschaftsstudien/eascy-five-trends-transforming-the-automotive-industry_2018.pdf.

KPMG INTERNATIONAL, 2019. 2019 Autonomous Vehicles Readiness Index. [en línea]. Ginebra, Suiza: KPMG International. [Consulta: 25 marzo 2019]. 136024-G. Disponible en: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf.

LAW FIRM GORODISSKY & PARTNERS, 2017. Data protection in Russian Federation: overview. *Gorodissk.com* [en línea]. [Consulta: 10 junio 2019]. Disponible en: http://www.gorodissky.com/publications/articles/data-protection-in-russian-federation-overview/.

MIKOLIC-TORREIRA, I., HENRY, R., SNYDER, D., BEAGHLEY, S., PETTYJOHN, S.L., HARTING, S., WESTERMAN, E., SHLAPAK, D.A., BISHOP, M., OBERHOLTZER, J., SKRABALA, L. y WEINBAUM, C., 2016. A Framework for Exploring Cybersecurity Policy Options. [en línea]. S.l.: [Consulta: 19 mayo 2019]. Disponible en: www.rand.org/t/RR1700.

MONTORO GONZÁLEZ ANA MARTÍ-BELDA BERTOLÍN IGNACIO LIJARCIO PATRICIA BOSÓ CONSUELO LÓPEZ, L. y VILADRICH CASTELLANAS JOSÉ SUÁREZ REYES, R., 2016. Coche Autónomo, seguridad vial y formación de conductores. [en línea]. Valencia: [Consulta: 2 mayo 2019]. Disponible en: https://www.cnae.com/ficheros/files/noticias/INFORME Coche autónomo seguridad vial y formación de conductores_ INTRAS-CNAE.pdf.

RAMÍREZ MORÁN, D., 2017. Ciberseguridad en China. *bie3: Boletín I.E.E.E., ISSN-e*

2530-125X, Nº 5 (enero - marzo), 2017, págs. 8-15 [en línea], no. 5, pp. 8-15. [Consulta: 13 junio 2019]. ISSN 2530-125X. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6057663.

RENTERÍA TAZO, A., 2017. Conectividad del vehículo y seguro: desafíos en la industria del automóvil. [en línea]. Madrid: Gómez-Acebo & Pombo. [Consulta: 28 abril 2019]. Disponible en: www.gomezacebo-pombo.com,.

SCHAUB, M. y ZHAO, A., 2018. China Issues Final Guidelines on Standards Establishment for Self-driving Cars. *King & Wood Mallesons Law Firm Web* [en línea]. [Consulta: 11 junio 2019]. Disponible en: https://www.kwm.com/en/knowledge/insights/final-guidelines-on-standards-for-self-driving-cars-20180109#id-here.

U.S. DEPARTMENT OF TRANSPORTATION, 2018. Automated Vehicles 3.0 Preparing for the Future of Transportation. [en línea]. Washington, DC: [Consulta: 28 abril 2019]. Disponible en: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

UNIÓN INTERNACIONAL, DE TELECOMUNICACIONES (UIT), EL BANCO MUNDIAL, la S. de la C., (COMSEC), LA ORGANIZACIÓN DE TELECOMUNICACIONES DE LA COMMONWEALTH (CTO), E. y CENTRO DE EXCELENCIA DE CIBERDEFENSA COOPERATIVA DE LA OTAN (CCDCOE OTAN), 2018. Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad. [en línea]. S.l.: [Consulta: 10 junio 2019]. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS Guide_s.pdf.

ZHAO, HOULIN; IBARAKI, STEPHEN; SAHOTA, NEIL; NARAIN, NIVEN R.; AKHTMAN, JOSEF; KHALDI, NORA; BROWNE, EMMET; HINCHEY, MIKE; WERNER, FREDERIC; BANIFATEMI, A., 2018. Nuevas fronteras reglamentarias. Cómo las tecnologías emergentes están dando lugar a enormes oportunidades y desafíos potenciales. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 24 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-03/2018_ITUNews03-es.pdf.

ZHAO, HOULIN;LANCTOT, ROGER; LEE, CHAESUB; HELLÅKER, JAN; FRANKLIN, L.I.N., 2018. La tecnología conduce los coches del mañana. *ITU News Magazine* [en línea]. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. [Consulta: 25 marzo 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-02/2018_ITUNews02-es.pdf.

ZHAO, H. y VECCHIONE, MAURIZIO;HERWEIJER, CELINE; STEWART, UYI; IBARAKI, STEPHEN; ZURUTUZA, NAROA; SAHOTA, NEIL; FENECH, MATTHEW; SALIBA, T., 2018. Inteligencia artificial para el bien del mundo. *ITU News Magazine* [en línea]. Ginebra: Unión Internacional de Telecomunicaciones. [Consulta: 14 junio 2019]. Disponible en: https://www.itu.int/en/itunews/Documents/2018/2018-01/2018_ITUNews01-es.pdf.

Anexos

No. 1 Niveles de Automatización de los Vehículos

Nivel	Denominación	Definición	Tareas de conducción		Conducción Longitudinal (Acelerar/frenar) y Lateral (Dirección)	Control del Entorno	Recuperación de las Tareas de Conducción en Caso de Contingencia	Tareas de Conducción realizadas por el Sistema
			Conductor	Sistema				
0	**Sin automatización**	El conductor realiza continuamente todas las tareas asociadas a la conducción, incluso cuando son mejoradas a través de algún aviso o la intervención de sistemas.	El conductor realiza continuamente la tarea de conducción dinámica lateral y longitudinal.	N/A	Conductor	Conductor	Conductor	N/A
1	**Conducción Asistida**	El sistema de ayuda a la conducción desarrolla una tarea específica, bien realiza la conducción dinámica lateral o longitudinal utilizando la información del entorno del vehículo, mientras que el conductor realiza el resto de las tareas de conducción.	El conductor realiza continuamente la tarea de conducción dinámica lateral y longitudinal.	El sistema realiza la conducción longitudinal o lateral que no esté realizando el conductor.	Conductor y Sistema	Conductor	Conductor	Algunas
2	**Conducción Parcialmente Automatizada**	El sistema de ayuda a la conducción desarrolla la conducción dinámica lateral o longitudinal utilizando la información del entorno del vehículo, mientras que el conductor realiza el resto de las tareas de conducción.	Supervisión de las tareas de conducción dinámica y el entorno.	Conducción longitudinal y lateral en un caso de uso definido.	Sistema	Conductor	Conductor	Algunas

3	**Conducción Automatizada Condicionada**	El sistema de conducción automatizada desarrolla todas las tareas de la conducción con la expectativa de que el conductor responda adecuadamente a la petición de intervención por parte de éste.	No es necesaria la supervisión constante de la conducción automatizada pero siempre debe estar en una posición adecuada para reanudar el control	Conducción longitudinal y lateral en un caso de uso definido. Reconoce sus límites de rendimiento y pide al conductor reanudar la tarea de conducción dinámica con margen de tiempo suficiente	Sistema	Sistema	Conductor	Algunas
4	**Conducción Altamente Automatizada**	El sistema de conducción automatizada desarrolla todas las tareas de la conducción, incluso si el conductor no responde adecuadamente a la petición de intervención por parte de éste.	El conductor no es requerido durante el caso de uso.	Conducción longitudinal y lateral en todas las situaciones de un caso de uso definido.	Sistema	Sistema	Sistema	Algunas
5	**Conducción Plenamente Automatizada**	El sistema de conducción automatizada desarrolla todas las tareas de la conducción bajo todas las circunstancias de la vía y ambientales.	N/A	Conducción longitudinal y lateral en todas las situaciones encontradas durante toda la prueba. No se requiere conductor.	Sistema	Sistema	Conductor	Todas

No. 2 Índice de Preparación para Vehículos Autónomos 2019

Ranking general	País	Total general
1	Holanda	25.05
2	Singapur	24.32
3	Noruega	23.75
4	EUA	22.58
5	Suecia	22.48
6	Finlandia	22.28
7	Reino Unido	21.58
8	Alemania	21.15
9	Emiratos Árabes Unidos	20.69
10	Japón	20.53
11	Nueva Zelanda	19.87
12	Canadá	19.80
13	Corea del Sur	19.79
14	Israel	19.60
15	Australia	19.01
16	Austria	18.85
17	Francia	18.46

18	**España**	**15.50**
19	**República Checa**	**14.46**
20	**China**	**14.41**
21	**Hungría**	**11.99**
22	**Rusia**	**8.55**
23	**México**	**7.73**
24	**India**	**6.87**
25	**Brasil**	**6.41**

Fuente: KPMG International 2019

No. 3 Elementos tangibles e intangibles de los Vehículos Autónomos

Fuente: McKinsey&Company

No. 4 Situación regulatoria de la protección de los datos personales en Latinoamérica

Fuente:

Deloitte. (2018). IoT para el Sector Empresarial en América Latina. Montevideo: Centro de Estudios de Telecomunicaciones de América Latina

No. 5 Listado de incidentes, eventos, alertas o noticias sobre la seguridad de los vehículos inteligente más relevantes ocurridos en los últimos años[171]

- **30/01/2015 La Asociación Automóvil Club Alemán (ADAC por sus siglas en alemán) publica una vulnerabilidad que afecta a los modelos de vehículos de BMW con el sistema ConnectedDrive y SIM propia de datos.** BMW ConnectedDrive permite utilizar un teléfono inteligente para abrir la cerradura de casi cualquier BMW, Mini o Rolls-Royce que venga equipado con esta característica. La vulnerabilidad encontrada en este sistema permitía acceder a datos e incluso abrir el vehículo. BMW procedió a la actualizando los coches afectados corrigiendo la grave vulnerabilidad en aproximadamente 2.2 millones de coches.

- **21/07/2015 Charlie Miller y Chris Valasek, especialistas e investigadores en ciberseguridad, logran hackear remotamente a través de Uconnect un Jeep Cherokee fabricado en 2014.** Este sistema fue instalado en cientos de miles de vehículos fabricados por el grupo Fiat Chrysler Automobiles (FCA) desde finales del 2013 y permite a sus propietarios encender remotamente sus coches, desbloquear las puertas, etc. Un fallo de seguridad facilita el acceso al sistema y realizar acciones como apagar el motor, controlar funcionalidades como el aire acondicionado, los cierres y la radio. Los investigadores notificaron este hecho a Fiat Chrysler el noviembre de 2014 permitiendo al fabricante desarrollar una actualización de seguridad para solucionar el problema. Los investigadores apreciaron que aparentemente no era posible actualizar de manera automática los coches a través de Internet por lo que los clientes debían actualizar manualmente accediendo a la página web del fabricante, descargando la actualización en un dispositivo externo e instalándola. Los investigadores estimaron que en ese momento había alrededor de 471.000 vehículos en circulación afectados por este fallo.

[171] Información tomada del sitio institucional del INCIBE-CERT https://www.incibe-cert.es/search/site/coches%20autonomos

- **14/08/2015 Se conoce que Volkswagen ocultó un grave fallo de seguridad durante dos años en los vehículos de esta propia marca, junto con otras de su grupo como Audi, Bentley, Porsche o Lamborghini.** Las vulnerabilidades se encontraban en el dispositivo de inmovilización Megamos Crypto que permitía arrancar el motor únicamente si la llave es la correcta; desde 2012 investigadores[172] descubrieron que este sistema de seguridad podía ser vulnerado por medio de un ataque de fuerza bruta y fueron capaces de reducir el número de combinaciones a 196 607 al interceptar la clave que se enviaba entre la llave del conductor y el dispositivo de inmovilización. Volkswagen demandó a los investigadores alegando que si la vulnerabilidad se hacía pública el número de robos aumentaría. Las medidas cautelares impuestas por el Tribunal Superior del Reino Unido impidieron que los resultados de su investigación vieran la luz hasta la conferencia de seguridad USENIX celebrada en Washington D.C en agosto de 2015.

- **18/09/2015 Se publica una vulnerabilidad sobre falta de autorización en el dispositivo de información y entretenimiento Uconnect fabricado por Harman-Kardon.** El sistema de información y entretenimiento Uconnect tenía acceso directo a algunos controles del vehículo, por lo que un potencial atacante que se hubiera conectado a este sistema podía tener control total sobre el dispositivo y enviar comandos a las unidades de control del vehículo, afectando tanto a la información mostrada (tacómetro) como a otros sistemas como los frenos o la dirección. La Fiat Chrysler Automobiles procedió a contactar voluntariamente a sus 1,4 millones de clientes para aplicar un parche que soluciona los problemas de UConnect.

- **24/02/2016 El investigador Troy Hunt anuncia un fallo de seguridad en la aplicación Nissan Connect EV instalada en los modelos eléctricos LEAF y EnV-200 de Nissan, que permitía a un atacante controlar el sistema de**

[172] Los investigadores fueron Flavio García, Baris Ege and Roel Verdult; el primero un profesor de ciencias de la computación en la Universidad de Birmingham en el Reino Unido, y los otros dos de la Universidad de Radboud en los Países Bajos, que encontraron un problema con el sistema Megamos Crypto utilizado en algunos autos, y creyeron que el público tenía derecho a saber sobre la debilidad de la seguridad.

climatización y la calefacción del coche. Asimismo esta vulnerabilidad permitía el acceso a información del ordenador de a bordo y obtener el número de bastidor del vehículo utilizando únicamente un navegador y una conexión a internet. La marca japonesa decidió suspender de forma temporal en sus coches eléctricos la aplicación por motivos de seguridad.

- **06/03/2016 Se hizo público la insuficiente configuración de seguridad de algunas TGU (Telematics Gateway Units) que se encontraban expuestas en internet, lo que amenazaba a los vehículos que las incorporaban, generalmente camiones.** A través de la TGU es posible ubicar el vehículo, obtener información de este y pone en riesgo otros sistemas del vehículo al estar conectada al bus CAN.

- **06/06/2016 Investigadores de seguridad consiguen vulnerar la seguridad del vehículo híbrido Mitsubishi Outlander PHEV.** A través de un ordenador portátil lograron acceder de forma no autorizada a varias de las funciones del vehículo, como encender o apagar las luces, desactivar la alarma antirrobo. Esto permitió el acceso al interior del vehículo a través de las ventanillas y una vez dentro acceder al puerto de diagnóstico que permite acceder a funciones vitales del coche. Mitsubishi procedió a trabajar para corregir este problema.

- **11/08/2016 Se conoce que un grupo de investigadores demostró la posibilidad de clonar a través de software y material informático de bajo costo los mandos de desbloqueo de puertas de más de 100 millones de vehículos fabricados por el grupo Volkswagen a partir del año 1995.** Utilizando un transceptor de radiofrecuencia basado en Arduino fue posible capturar el código de las llaves, descifrar sus códigos y generar un duplicado que posteriormente permitiera abrir el vehículo que se encontraron en peligro.

- **20/09/2016 La empresa de seguridad china Keen Security Lab publica un video en el que se muestra como el coche eléctrico Tesla Modelo S podía ser controlado de forma remota.** En las pruebas realizadas por los investigadores se

mostró como se podían accionar de forma remota los frenos del coche, abrir el coche, mover los asientos o controlar la pantalla del Tesla. Estas vulnerabilidades fueron comunicadas a la compañía Tesla que procedieron a trabajar en una actualización.

- **06/06/2017 Investigadores de la compañía Kromtech Seguridad descubren una base de datos desprotegida que contenía datos de varios concesionarios de automóviles con sede en Estados Unidos, resultando en una exposición de la información de 10 millones de propietarios de coches en el país.** La base de datos revelaba datos personales de los compradores como nombres, direcciones, números de teléfono, fecha de nacimiento, sexo e hijos mayores de 12 años. Además incluía detalles de ventas como número de bastidor, kilometraje, modelo, año del modelo, tipo y cantidad de pago mensual y nombre del comercial. Los datos filtrados estuvieron en línea 137 días y la identidad del propietario de la base de datos no fue conocida. Los grupos especializados en el robo de vehículos podrían usar esta información para clonar el número de bastidor y hacer que un coche robado parezca legal a la hora de realizar su venta.

- **28/07/2017 Los investigadores Mickey Shkatov, Jesse Michael y Oleksandr Bazhaniuk del Advanced Threat Research Team de McAfee descubrieron dos vulnerabilidades relacionadas con la gestión de la memoria en diversos modelos de vehículos que utilizaban el módulo de control telemático Infineon S-Gold 2 (PMB 8876) de Continental AG.** Un potencial atacante pudo haber aprovechado estas vulnerabilidades para ejecutar código arbitrario en el procesador de radio de banda base de la TCU, permitir deshabilitar el sistema de infotainment (sistema de información y entretenimiento) y afectar a características funcionales del vehículo vinculadas en el Identificador Temporal del Abonado Móvil (TMSI) permitiendo a un atacante el acceso y control de la memoria. Las vulnerabilidades permitían igualmente a un atacante con acceso físico al TCU (módulo de control telemático) explotar un desbordamiento de búfer que existe en el procesado de comandos AT. En su momento no existió ningún plan de mitigación por parte de Continental AG. Nissan e Inifinity propusieron a los

usuarios contactar con su vendedor local para desactivar el módulo TCU 2G afectado. Ford mediante su programa de satisfacción de clientes ofreció la actualización o deshabilitación de los viejos módems 2G. BMW, por su parte, analizó las vulnerabilidades y ofreció una solución a sus clientes.

- **31/07/2017 Los investigadores Andrea Palanca, Eric Evenchick, Federico Maggi y Stefano Zanero identificaron una debilidad en el protocolo CAN Bus que pudo permitir a un potencial atacante realizar una denegación de servicio.** Una modificación específica de los bit dominantes y recesivos de la trama CAN pudo suponer que un atacante con acceso físico a un dispositivo que usara el protocolo y con extenso conocimiento de este, realizar una denegación de servicio afectando a la disponibilidad de funciones arbitrarias dentro del dispositivo objetivo. La única recomendación que en su momento se comunicó para protegerse de la vulnerabilidad fue limitar el acceso a los puertos de entrada, especialmente al puerto ODB-II, en automóviles. Se trabajó en la búsqueda de mitigaciones.

- **21/09/2017 Es víctima de un ciberataque a sus servidores la compañía estadounidense SVR Tracking dedicada a monitorizar la señal GPS[173] de vehículos para hacer su seguimiento, alertar de sus movimientos y de esta manera recuperarlos en caso robo, lo cual provocó el robo de información sensible de más de 500.000 clientes.** Entre los datos que fueron sustraídos se encontraba el nombre de usuario y la contraseña de la plataforma web, el número de identificación del vehículo, el IMEI[174] del dispositivo GPS, e incluso la localización oculta de este dispositivo en el vehículo. El ciberataque se llevó a cabo debido a que la compañía disponía de un servidor cache sin contraseña, y en el que se alojaban todos estos datos; además, las contraseñas sustraídas se

[173] El Sistema de Posicionamiento Global (Global Positioning System en inglés) es un sistema que funciona mediante una red de satélites en órbita sobre el planeta Tierra que permite determinar la posición de cualquier objeto o persona; fue desarrollado, instalado y empleado por el Departamento de Defensa de los EUA.
[174] La Identidad Internacional de Equipo Móvil (International Mobile Equipment Identity en inglés) es un número de 16 dígitos que identifica a cada dispositivo móvil, con el IMEI se puede saber el fabricante, el modelo y el número de serie del equipo móvil.

protegían mediante el algoritmo de cifrado SHA[175]-1, que ya era obsoleto en esa fecha debido a su facilidad para descifrarlo.

- **21/12/2017 La firma nipona de automóviles Nissan informó una posible fuga de información acaecida en su filial canadiense de financiación de vehículos tanto de Nissan como de Infinity, su marca de lujo.** En total, alrededor de 1,1 millones de usuarios de la financiera se vieron afectados por este robo de información del cual, entre otros datos, fueron sustraídos nombres de compradores, domicilio y número de identificación de los vehículos; sin embargo, la compañía informó en ese momento que no había indicios de que se hubieran filtrado números de teléfono ni de direcciones de correo electrónico. Se continuó investigando el incidente y el impacto que pudo tener en usuarios fuera de Canadá.

- **13/11/2018 El investigador de seguridad Bob Diachenko descubre una base de datos de usuarios de Kars4Kids, organización de donación de coches sin fines de lucro, sin ningún tipo de protección que contenía 21.612 registros con detalles personales.** Los datos estaban disponibles desde múltiples instancias de MongoDB mal configuradas, que incluían información relativa a direcciones de correo electrónico y datos personales, además de credenciales para el inicio de sesión con privilegios de administrador. Bob Diachenko contactó con Kars4Kids para informarles de la vulnerabilidad de seguridad, y le respondieron que securizaron la base de datos vulnerable, notificaron el incidente al Buró Federal de Investigaciones de EUA (FBI) e informaron a los donantes cuya información se vio afectada.

[175] El Algoritmo de Hash Seguro (Secure Hash Algorithm en inglés) es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Normas y Tecnología, INNT (NIST en inglés) de los EUA.