Anuario da Facultade de Dereito da Universidade da Coruña
Vol. 28 (2024), pp. 65-92
ISSNe: 2530-6324 || ISSN: 1138-039X
DOI: https://doi.org/10.17979/afdudc.2024.28.10234

RESPONSABILIDAD CIVIL EN VEHÍCULOS AUTÓNOMOS Y SOLUCIONES JURÍDICAS DE LA LEY DE INTELIGENCIA ARTIFICIAL (AI ACT)

CIVIL LIABILITY IN AUTONOMOUS VEHICLES AND LEGAL SOLUTIONS IN ARTIFICIAL INTELLIGENCE RULES (AI ACT)

ENRIQUE VÁZQUEZ PITA
Doctorando en el Programa de Derecho y Ciencias Sociales de la UNED
https://orcid.org/0000-0001-5541-9835

Recibido: 29/12/2023
Aceptado: 09/07/2024

Resumen: Los problemas teóricos sobre la responsabilidad civil para compensar los daños generados por los coches autónomos (AVs), actualmente en desarrollo, se han intentado resolver aplicando soluciones utilitaristas como el «dilema del tranvía» y recurriendo a la legislación penal de accidentes de tráfico, la cual dentro de unos años se verá superada por un nuevo ecosistema tecnológico que requiere normativas más profundas que los cuatro niveles de riesgo de la *AI Act* (AIA) de la UE. El presente artículo propone abordar estos conflictos legales con una visión del Derecho que considere al coche autónomo como un robot que opera con Inteligencia Artificial (IA). Otra recomendación es aplicar a los AVs la legislación actual sobre derechos humanos (privacidad, intimidad, discriminación, ciberataques, imprevisibilidad, opacidad).

Palabras clave: coche autónomo, Inteligencia Artificial, responsabilidad civil, daños, AI Act

Abstract: The theoretical problems regarding civil liability to compensate for the damages generated by autonomous cars (AVs), currently under development, have been attempted to be resolved by applying utilitarian solutions such as the «tram dilemma» and resorting to criminal legislation for traffic accidents, the which in a few years will be surpassed by a new technological ecosystem that requires deeper regulations than the four risk levels of the EU AI Act. This article proposes to address these legal conflicts with a vision of Law that considers the autonomous car as a robot that operates with Artificial Intelligence (AI). Another recommendation is to apply current legislation on human rights (privacy, intimacy, discrimination, cyber attacks, unpredictability, opacity) to AVs.

Keywords: Artificial Intelligence, civil liability, AI Act, damages, autonomous cars (AVs)

* * *

I. PLANTEAMIENTO

El mundo jurídico se halla ahora ante una transición de la normativa donde el nuevo combustible son los datos y la inteligencia artificial (IA). La Dirección General de Tráfico inició en 2023 la construcción de un marco regulatorio del coche autónomo de niveles 4 y 5 SAE (100% autónomos) que pretendía tener listo para el año 2024, a través del Real Decreto de Circulación de Vehículos Autónomos, que, previsiblemente, modificará el Reglamento de Circulación y el Reglamento General de Vehículos. Supondrá un cambio radical en las ciudades inteligentes (*smart-cities*) y la extracción de datos del tráfico y obligará a habilitar espacios de ensayo, una figura recogida en la *AI Act* o Ley de Inteligencia Artificial para probar sistemas de IA de alto riesgo (porque afectan a la seguridad) en condiciones del mundo real fuera de los espacios aislados de regulación de la IA. El Anexo III punto 2 de la *AI Act* incluye como sistemas de IA de alto riesgo a los destinados a ser utilizados como componentes de seguridad en la gestión y explotación de tráfico rodado. Otros países, como el Reino Unido, aprobaron en noviembre de 2023 un nuevo reglamento para el coche autónomo (*Automated Vehicles* [AV] *Bill*). Probablemente, estas normas inaugurarán una nueva ramificación legal no solo respecto a la seguridad vial sino también en la emergente disciplina del Derecho de la IA. Actualmente, no hay coches totalmente autónomos pero en California, por ejemplo, ya rueda el servicio de robotaxis de Cruiser, y que en septiembre de 2023 perdió su permiso de circulación al arrollar a una viandante tendida en la calzada. Estados Unidos se plantea prohibir los coches eléctricos chinos BYD por sospechar que recogen datos sensibles con sus sensores.

La clave para el Derecho es que a, diferencia de los agentes virtuales, el coche autónomo es una máquina cuyo comportamiento influye en su entorno físico y puede causar daños reales y cuantificables para los usuarios del vehículo y terceros, lo que genera responsabilidades. Pero como se mostrará en el Capítulo III del presente artículo, el coche autopilotado también ha de considerarse como una máquina de ocio multimedia, un nuevo espacio o entorno de consumo de ocio y de producción (ese tiempo ahorrado en la conducción

se “optimizará” para consumo o como oficina móvil) que facilitará la extracción de datos personales y planteará nuevamente conflictos de privacidad e intimidad que se intentarán resolver aplicando el Reglamento General de Protección de Datos y el Proyecto Final Completo de la *AI Act* aprobado por el Consejo de la UE el 21 de mayo de 2024, pendiente de su entrada en vigor escalonada.

El proyecto para desarrollar el coche autónomo sin conductor (un coche eléctrico dotado o autodirigido mediante IA) podría mejorar la seguridad en las carreteras europeas aunque, desde la perspectiva del Derecho, como se abordará en este artículo, genera problemas jurídicos a la hora de resolver cuestiones como la responsabilidad civil por daños causados a terceros por posibles lagunas en la legislación actual. El reglamento de la *AI Act* o Ley de la Inteligencia Artificial introduce la figura del implantador (antes implementador), a efectos de responsabilidad, y prevé cuatro niveles de riesgo, una clasificación en la que los robots industriales (se entiende que es extensible a los vehículos autónomos), por sus problemas de seguridad, son considerados como de alto riesgo. La pretensión es que los coches autónomos eliminen el error humano en la carretera, dado que los despistes, la somnolencia o la ingesta de bebidas alcohólicas provocan el 95 % de los accidentes mortales en las carreteras de la UE. Por los viales del viejo continente circulan a diario 246 millones de coches, de los que el 1,1 % son eléctricos (casi 4 millones de coches enchufables). No obstante, dado que estos coches autopilotados circularán conectados en tiempo real a una red central en la Nube (una infraestructura digital crítica, según la *AI Act*) no se descarta que haya “apagones” o averías que paralicen cientos o miles de coches simultáneamente y causen grandes atascos o accidentes graves.

La UE pretende que haya 30 millones de coches eléctricos en Europa en 2038 pero esa meta genera escepticismo en el sector de la industria del motor por problemas técnicos. La implantación del coche autónomo podría reducir las ratios de mortalidad de tráfico si va acompañado de mejoras en las infraestructuras, como por ejemplo, la habilitación de un carril exclusivo para la circulación de vehículos eléctricos que va a implantar Suiza o las líneas de dirección de carril, que propone el Reino Unido. En ese sentido, un informe del Ministerio de Transportes británico del 2022, que recomienda instalar *Automated Lane Keeping Systems* (ALKS) o sistemas automatizados de mantenimiento de carril, argumenta que los coches autónomos y otras innovaciones como los robot-taxis harán más segura la carretera porque la IA reducirá el número de errores humanos y, en consecuencia, rebajará los accidentes y colisiones.

La IA, hasta el 2024, estaba regulada en la UE a través de las leyes sobre productos defectuosos aunque, para los coches autónomos, ATIENZA NAVARRO ve más ventajosa para la víctima la aplicación de la responsabilidad civil por daños causados por vehículo a motor (LRCVCM). La puesta en marcha del coche autónomo es compatible con el compromiso de la Administración europea con su hoja de ruta para reducir a cero los accidentes de tráfico en el 2050 (Proyecto Visión Cero). Pero aunque la UE intente minimizar los daños, será difícil que haya cero accidentes. No hay que olvidar que la IA es un agente

con cierto grado de autonomía que genera acciones con consecuencias en la vida real. El conflicto legal surgirá con máquinas totalmente autónomas de nivel 4 y 5, y cuya operatividad necesitará de ir acompañada de un nuevo ecosistema de infraestructuras como el 6G porque el actual 5G no es lo bastante potente para que el coche reaccione en tiempo real), nueva señalización y los carriles especiales para coches autónomos.

1. Los vehículos autónomos y el Derecho

Los problemas causados por los vehículos autónomos, también denominados AVs, obligarán a redactar una nueva arquitectura legal que requerirá una regulación global o transnacional, siguiendo la línea marcada por *Meneceur*. El término «arquitectura» se está usando para el diseño de software y todo el ecosistema digital y, por analogía, este artículo propone extenderlo al diseño de un nuevo armazón legal que soporte los cambios que traerá la IA y cuyos pilares básicos son la RGPD y la *AI Act*.

El presente artículo abordará el estudio de la responsabilidad civil en caso de accidente o daños causados por los AVs dentro de este escenario de vacío legal. Las partes en conflicto deben asumir que los coches autopilotados son una pieza más de un ecosistema triangular dominado por la IA, un sistema de telecomunicaciones de banda ancha 5G (y en un futuro, 6G) que permite una interacción de la máquina con otros objetos en tiempo real (baja latencia), Internet de las Cosas y la robótica. Este escenario presenta altos riesgos tecnológicos asociados a la IA, especialmente en los niveles 4 y 5 de la conducción autónoma. Como se verá más adelante, la previsible explotación de los datos del conductor y los ocupantes enlaza directamente con los riesgos altos (reconocimiento biométrico, registro de emociones) descritos por el Proyecto Final de la *AI Act* del 21 de mayo de 2024 y ya previstos en el apartado 10 del Reglamento (UE) 2019/2144, que establece que cualquier de los sistemas de seguridad debe funcionar sin utilizar ningún tipo de información biométrica sobre conductores, pasajeros, incluidos los de reconocimiento facial. Todo ello requerirá un ensayo para la homologación de estos vehículos.

Entre dichos riesgos cabe citar la seguridad, responsabilidad, privacidad, ciberseguridad e influencia en la industria (desempleo), fundamentos recogidos en el espíritu de la *AI Act*. A esto se añade el llamado «dilema social» de los AVs cuando adoptan decisiones de forma autónoma en un accidente inevitable que genera daños y responsabilidad civil y sobre lo que la *AI Act* no propone expresamente una solución salvo la realización de ensayos y experimentos previos de los prototipos de IA. Como otras tecnologías basadas en la IA, innovaciones como el coche autónomo presentan lagunas e incertidumbres jurídicas. La solución ha consistido en adaptar los nuevos casos que surgen al arsenal ya existente de leyes sobre responsabilidad, y los principios del derecho y derechos fundamentales.

En la misma línea, el presente artículo pretende visibilizar ante los estudiosos del Derecho y los legisladores, los nuevos retos de los coche-robot y el Derecho civil, así como la estimación de sus riesgos y consecuencias en la responsabilidad por daños. Aunque los

coches autónomos tardasen una o dos décadas en circular por las carreteras, los problemas jurídicos que los juristas están abordando ahora servirán para entender cómo funciona el nuevo ecosistema de la IA y sus riesgos y sugerir soluciones.

La primera parte del artículo establece la conexión entre IA y vehículo autónomo y sus problemas asociados. En un segundo apartado, se aborda el progreso en la legislación sobre vehículos autónomos y la realización de pruebas y test y su circulación en carreteras, así como los proyectos de *soft law* que se han propuesto. En la tercera, se analizan los esfuerzos teóricos para resolver dilemas éticos como el del tranvía. En una cuarta parte, se estudian las dificultades doctrinales para distribuir la responsabilidad civil por los daños causados por los AVs, habida cuenta de la complejidad del ciclo de producción y lo imprevisible que es el ecosistema de la IA.

La atribución de responsabilidades civiles de los AVs en caso de accidente solo ha sido jurídicamente resuelta con la *AI Act* del 2024. Hasta entonces, se podía calificar de laguna legal, según reconoció en su día la UE en su Libro Blanco sobre la IA. El borrador de la *AI Act* (AIA) tampoco asumía el problema, más allá de calificar aquella IA que genere problemas de seguridad como IA de alto riesgo o de riesgo inaceptable, cuestión que zanja el texto final del 2024 al atribuir responsabilidades a cada uno de los intervinientes de la cadena. Las propuestas que están llamando la atención a los juristas son, por contra, las normas que sugiere la Comisión Europea para evitar que el sesgo algorítmico conduzca a la discriminación o la propuesta de crear un proceso de certificación para usos de inteligencia artificial de alto riesgo. Apréciese que la cuestión no es baladí, toda vez que ya hay accidentes mortales causados por AVs como, por ejemplo, un arrollamiento de una mujer tendida en la calzada causado por un robo-taxi en septiembre de 2023 y que llevó al Departamento de Vehículos Motorizados de California (DMV) a suspender los permisos de circulación sin conductor a la empresa Cruise en San Francisco. Hay otros casos. Por tanto, todo ello evidencia la potencial concurrencia de la responsabilidad civil en este tipo de coches-robot, en un momento en que la tipificación normativa aún es objeto de estudio y análisis. La NTSB y los 50 estados de Estados Unidos tienen por delante el reto de armonizar su regulación respecto a los coches autónomos. La pandemia del covid-19, en 2020 y 2021, afectó negativamente al negocio del coche autónomo como vehículo inteligente compartido. Si el vehículo fuese de uso individual, el resultado sería bien diferente.

2. La conexión de los IA y los Avs

El factor clave de los coches autónomos (AVs) es que funcionan con IA. La UE así lo reconocía en su Libro Blanco sobre la IA, en el que definía la Inteligencia Artificial como un término que se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos. La UE reconoce la conexión entre automóvil autónomo y la IA al señalar que los sistemas basados en la IA pueden consistir simplemente en un programa informático (asistentes de voz, programas de análisis de imágenes, motores de

búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware [robots avanzados, automóviles autónomos, drones o aplicaciones del Internet de las Cosas (IoT)]. Otra aplicación de la IA es la predicción de las trayectorias en los carriles.

El coche autónomo ligado a la IA puede beneficiarse del aumento exponencial de la capacidad de aprendizaje. Sin embargo, también sus riesgos son de crecimiento ultrarrápido e imprevisibles. La conducción autónoma está fundada tanto del aprendizaje automático, alimentado de bases de datos (*big data*) adoptados de conducciones reales en la carretera y de entrenamientos y del tratamiento como de la identificación de imágenes y reconocimiento de patrones. Pese al escepticismo actual, los AVs previsiblemente circularán por las carreteras y, cuando llegue el momento, los legisladores deberían de haber aprobado un arsenal de fórmulas para distribuir la responsabilidad civil por daños personales o patrimoniales causados por coches sin conductor. En este aspecto, la ausencia de previsión y programación previa normativa hace suponer que existirá un grave vacío legal. Es probable que se repitan los errores debidos a la falta de regulación de la propiedad intelectual al nacer Internet o con el entrenamiento de ChatGPT o el ataque a la privacidad desde las redes sociales para hacer minería de datos. Si el hecho conflictivo existe, el Derecho ha de intervenir y estar disponible para resolverlo.

La relación entre IA y coches autónomos ha captado la atención de autores como YIFANG, ZHENYU, HONG, y LIN, quienes analizan cómo la IA da soporte a las principales aplicaciones en los AVs sobre percepción, localización, mapeo y toma de decisiones, lo que genera desafíos y problemas asociados con su implantación. No ignoran que la IA también puede aportar tecnologías emergentes como los mapas de alta definición, el *big data* y la computación de alto rendimiento, una plataforma de simulación mejorada de realidad aumentada (AR) y realidad virtual (VR) y una comunicación en 5G para los coches autónomos conectados. Hay tal interconexión con la IA que los AVs forman parte de un Sistema de Transporte Inteligente. La UE recuerda que, en el 2020, el 80% del procesamiento y análisis de datos que tenía lugar en la Nube se producía en centros de datos e instalaciones informáticas centralizadas, y el 20% en objetos conectados inteligentes, como automóviles, electrodomésticos o robots de fabricación, y en instalaciones informáticas cercanas al usuario (*edge computation*). Según la Comisión Europea, para el 2025, estas proporciones cambiarán notablemente.

Que los coches autónomos funcionen con IA implica inseguridad y lagunas legales relacionadas con la existencia de algoritmos opacos y con el análisis masivo de datos por parte de plataformas y grandes redes interconectadas, no solo mediante *big data* sino también con las comunicaciones a través de GPS y satélites, la llamada geolocalización. La primera generación de toma de decisiones predictivas de la IA, según expone AGRAWAL se basaba en el siguiente algoritmo «*If/Then*» (si... entonces), lo que permite que un coche autónomo frene si detecta un obstáculo en el camino. Sin embargo, la segunda generación se basa en esta pregunta: «¿Qué haría un humano?», lo que conlleva la extracción de datos de los

conductores, para retroalimentar una base de datos que mejora el software de conducción autónoma mediante aprendizaje profundo (*Deep Learning*), lo que supone una falta de privacidad.

Los problemas asociados a la IA se agolpan y, por ende, afectan al desarrollo del coche autónomo. Tal y como reconocía la UE en su Libro Blanco sobre la IA, las máquinas inteligentes toman decisiones de forma opaca (el «efecto caja negra» o black box) o sus itinerarios lógicos para obtener un resultado son ininteligibles para el ser humano (el *deep learning* o aprendizaje profundo o automático sopesa miles de parámetros). En concreto, la UE advierte que la opacidad, la complejidad, la imprevisibilidad y un comportamiento parcialmente autónomo, «pueden hacer difícil comprobar el cumplimiento de la legislación vigente de la UE sobre la protección de los derechos fundamentales e impedir su cumplimiento efectivo. Puede ser que las fuerzas y cuerpos de seguridad y las personas afectadas carezcan de los medios para comprobar cómo se ha tomado una decisión determinada con ayuda de la IA y, por consiguiente, si se han respetado las normas». En este sentido, faltaría el requisito de nexo de causalidad para atribuir la responsabilidad civil, algo que ya ha sido detectado por autores que estudian los daños causados por sistemas autónomos. La solución planteada por la UE consiste en dar cierta ventaja probatoria al usuario para no generarle indefensión ante los grandes fabricantes y desarrolladores.

La UE reconoce que la tarea de los algoritmos es clave en la conducción automática porque usa, en tiempo real (baja latencia), los datos del vehículo (velocidad, consumo del motor, amortiguadores y otros) y de los sensores que examinan el entorno global (carretera, señales, otros vehículos, peatones, y otras variables) para determinar qué dirección tomar o qué aceleración y velocidad requiere el vehículo para llegar a un destino prefijado. A partir de los datos observados, el algoritmo se adapta a la situación de la carretera y las condiciones exteriores, como el comportamiento de otros conductores, para ofrecer la conducción más cómoda y segura posible. Otros riesgos surgen de errores en la programación o el jaqueo. La Comisión Europea identifica como riesgos de la IA la toma de decisiones opaca, la discriminación por género y de otros tipos, la intrusión en nuestra vida privada o su uso para propósitos criminales.

La legislación sobre la responsabilidad civil de los daños ocasionados por los coches autónomos, por tanto, va ligada a la regulación de la IA y exige comprender los riesgos que esta genera. Y, precisamente, la regulación de la IA, pieza clave del coche autopilotado, es una de las principales trabas, según reconoce el informe de España Digital 2025, asuntos que el Gobierno español considera que van a estar en la mesa de los líderes mundiales en los próximos años. Entre los objetivos de la Comisión Europea está dar cobertura 5G en el 2025 a las principales vías de comunicación y los corredores de transporte transfronterizos y, posteriormente, la 6G. El propio informe España Digital aboga por una transformación del modelo de movilidad para hacerlo sostenible, innovador y eficiente, impulsando la innovación y la colaboración multisectorial.

Los autores se dividen entre las bondades de los coches autónomos y eléctricos y los escépticos o detractores. BURNS dice que el coche de gasolina causa grandes problemas: alto consumo de combustible y de forma ineficiente (solo el 30% se usa para moverse), el 95 % del tiempo están parados, la ocupación es baja (1,7 personas por vehículo). Apuesta por rediseñar el ADN de los coches al estilo del GOOGLE'S CHAUFFER SELF-DRIVING CAR PROJECT, ahora Waymo. Eso requeriría cambios como una propulsión por células de hidrógeno, batería y biofueles. Diversas compañías de Silicon Valley se han lanzado a diseñar estos prototipos: Tesla, Lyft, Uber y Google-Waymo. En China, destaca en esta carrera *Tencent Holdings, Bejing Automotive* y BYD. En la misma línea LIPSON canta las bondades de lo que llama el robotic chauffer (chófer robot). WOLMAR y DIXON, que estudian desde hace años la industria del coche autónomo, se han vuelto escépticos sobre el desarrollo de esta tecnología.

DIXON es otra de las escépticas que propone usar el término de *autonowashing* para que el consumidor entienda las capacidades reales de los AVs y se evite la confusión del público a la vez que permite reflexionar sobre sus interacciones de seguridad.

3. Normativa comparada en materia de coche autónomo: definición técnica, pruebas y test vs. soft law

Con la llegada del vehículo a motor, la legislación sobre carruajes de tracción animal tuvo que ser actualizada. Las palabras carruaje y caballerías aún perviven en el artículo 346 del Código Civil español sobre bienes muebles e inmuebles pero el artículo 10.2 se refiere ya a automóviles, y el artículo 3.1 establece que las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativo y la realidad social del tiempo en que han de ser aplicadas. A mayores de estos arreglos, surgieron nuevos códigos legales (como el de Tráfico, Tributos especiales sobre la gasolina, señalizaciones, el Código de Viena de 1968, las emisiones de gases contaminantes) para adaptar las leyes a un mundo de vehículos a motor, sus combustibles y sus infraestructuras.

El mismo conflicto de obsolescencia plantea el término «conductor», que los códigos, al menos en España, asocian a una «persona». El asunto ha sido estudiado por Lozano, Cristina, que hace notar que el Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, había incluido un contenido que «quedaría obsoleto» con la introducción en la circulación de los vehículos autónomos, debido a que «el texto legal parte en todo momento de la idea de que exista un conductor llevando los mandos del vehículo». Aporta otros ejemplos de artículos que no contemplan la posibilidad de un vehículo autopilotado (los números 10, 11, 13 y Anexo 1), que establecen obligaciones para los conductores (uso con precaución, deber de identificación, la persona que maneja los mandos), a los que asimila solo con personas. La alusión al coche autónomo figura en la Instrucción 15/V-113 de la Dirección General de Tráfico para la autorización de pruebas o ensayos de investigación

realizados con vehículos de «conducción automatizada» en vías abiertas al tráfico en general y la a Instrucción 10/TV-66, para autorizar pruebas a fabricantes.

Argumentos como estos apoyan la idea de una nueva arquitectura legal que agrupe a todo el entorno de la IA. El coche autónomo o el *smart-car* generarán ramas emergentes como las recargas de vehículos eléctricos, taxis, uso compartido de coche y plazas de aparcamiento. Pero, en un mundo interconectado, se añaden todos los riesgos de la IA ya mencionados, que afectan a derechos fundamentales como la privacidad, y la no discriminación, que se vulneran a través de la opacidad o el sesgo algorítmico, entre otros, por no hablar de la ciberseguridad.

Todo apunta a que la irrupción del vehículo autónomo supondrá un nuevo escenario de conflictos y responsabilidades que, previsiblemente, requerirá ajustes en la legislación sobre infraestructuras o incluso la elaboración de una normativa específica cuando no se puedan dirimir los conflictos con los códigos actuales. La doctrina de en Francia, Estados Unidos o España, entre otros países, está analizando los posibles conflictos y grados de responsabilidad que pueden surgir en torno a este tipo de vehículos futuristas que se guían mediante algoritmos alimentados por análisis de datos y predicciones sobre el comportamiento y la conducta del usuario. Al estar encuadrados en un sistema digitalizado, eso precisamente, los hace vulnerables a los ataques informáticos de jáqueres, lo que abre otra vía para la reclamación por los daños ocasionados a causa de las brechas en la ciberseguridad de los vehículos.

Los principales avances en legislación sobre AVs se han obtenido en la definición técnica y graduación del coche autónomo y la normativa sobre las pruebas y test en carreteras públicas. Una tercera vía ha sido el *soft law*, adoptado por la UE y los autores que defienden códigos deontológicos para los conductores. El desarrollo legislativo sobre estos vehículos autopilotados arranca en la segunda década del siglo XXI con los primeros reglamentos en diversos países para garantizar la seguridad de las pruebas y test de rodaje de estos vehículos en las carreteras, fuera de pistas aisladas o de circuitos especialmente diseñados en las fábricas. La *Society of Automotive Engineers* (SAE) ha distinguido hasta cinco niveles de automatización en un vehículo-robot (desde el apoyo a la navegación a la conducción totalmente autónoma), lo que es un avance para establecer varios tipos de responsabilidades: en cascada, vicaria, o por negligencia profesional. Sin olvidar a los autores que apuestan por una hoja de ruta de *soft law* que aboga por establecer códigos éticos para los programadores y diseñadores del software de IA, basados en su moralidad y en la filosofía utilitarista (el mayor bien para el mayor número de personas). La SAE clasifica los coches autónomos (AVs) en cinco grados de menor a mayor autonomía del vehículo y, como señalan NOGUÉRO y DIXON, los fabricantes aún están trabajando en los protocolos para los niveles 2 y 3. Esta definición de los cinco niveles de la SAE ha sido adoptada, según TAEIGHAH y LIM en los cuerpos jurídicos nacionales e internacionales de la *Australia's National Transport Commission* (NTC), el Department for Transpo*rt* (DfT) del Reino Unido, la *National Highway Traffic Safety Administration* (NHTSA) de Estados Unidos, el Gobierno

de Ontario (Canadá) y por la Comisión Europea en su *Road Transport Research Advisory Council* (ERTRAC), entre otros.

La regulación de varios países anglosajones, como el Reino Unido o Estados Unidos, aborda cómo realizar los tests o pruebas de los prototipos en las vías públicas de los AVs, pero la legislación todavía debe afrontar aspectos jurídicos necesarios para que el coche autónomo pueda rodar por las carreteras. Algunos autores consideran preciso resolver la dicotomía entre los derechos IRL (*In Real Life* o reales) y los derechos en línea, definir el grado o nivel de automatismo (hay avances en el Reino Unido, EE.UU., la UE), aclarar las responsabilidades entre actores públicos y privados, y determinar cuándo se debe aplicar la responsabilidad en cascada y la responsabilidad in educando (atribuirla al entrenador del programa de IA). A ello, se suman otras materias jurídicas que surgen con la regulación de la IA como la obligación o recomendación de proteger los datos del usuario, estandarizar los *smart-contract*s (basados en la tecnología *blockchain*) para compartir un vehículo, regular el pago de servicios del coche autónomo con criptomonedas, prevenir la ciberdelincuencia, despejar el modelo de comunicación de vehículo a vehículo (V2V) y la comunicación entre vehículo e infraestructura (V2I). Un dilema que plantea la regulación de las industrias innovadoras, entre las que se encuentra el coche autónomo, es, siguiendo a Lessig, Lawrence, si su desarrollo legislativo debe seguir la máxima de *Code is law* (tiene prevalencia el código de la máquina) o su contraria, *Law is code* (donde prima la legislación).

La legislación sobre esta tecnología de coches conectados avanza en los países anglosajones, China, Singapur o Estonia. Hay instituciones que adaptan las novedades a sus leyes ya existentes o hacen estas más «inclusivas», caso del Reino Unido, o que se centran en la ciberseguridad, como Estados Unidos. Por contra, MENECEUR anima a generar una nueva regulación específica sobre IA porque ve difícil encaje en la existente y propone una legislación global sobre IA que esté unificada a fin de no dejar cabos sueltos (gaps) que dejen impunes las irregularidades como, en su día, ocurrió con los paraísos fiscales o los monopolios surgidos de Internet (los GAFAM). A un problema global se le debe dar una regulación global, defiende este magistrado. Le preocupan los fallos de seguridad.

TAEIHAGH y LIM dividen en cinco las estrategias seguidas por los gobiernos al legislar sobre riesgos y amenazas potenciales de los coches autónomos: ignorarlos, suprimirlos, controlarlos, tolerarlos o adaptarlos. Otras estrategias que sí figuran en la *Act AI*, consiste en controlar a los AVs mediante políticas y regulaciones que predicen los riesgos (caso de Singapur y su *Road Traffic Act*, que obliga a pasar test).

Parte de la doctrina sobre el coche autónomo como una rama de la IA, intenta resolver estos retos legislativos mediante propuestas para desarrollar una regulación no vinculante (*soft law*) o de soluciones éticas para los programadores. Esta táctica evita entorpecer el desarrollo tecnológico de un sector industrial estratégico. Surgen propuestas como que las grandes compañías se autorregulen (el lema de Google de «No seas malvado») o redactan códigos éticos o deontológicos que deben cumplir los programadores para evitar que su

despido sea procedente si se niegan a escribir un programa ilegal. La misma vía del soft law siguió la Comisión Europea, que elaboró directivas no vinculantes para el desarrollo de la Inteligencia Artificial y el Libro Blanco en el 2020 sobre dicha tecnología con recomendaciones para proteger al consumidor y generar un ecosistema de confianza. Otra vía es buscar el encaje de la IA en la legislación actual sobre derechos humanos (derecho a la privacidad, dignidad, no discriminación). Pero, como ha resaltado MENECEUR el soft law es una solución descafeinada porque ni el infractor está sujeto a sanciones ni los actores sujetos a obligaciones, como sí ocurre con las normas jurídicas.

En el caso de la UE, ha optado por una estrategia de *soft-law* a través de la publicación de un Libro Blanco de la Inteligencia Artificial, un enfoque europeo orientado a la excelencia y la confianza, luego desarrollado en el borrador de la *AI Act* (AIA) y, en el 2024, implementó un texto final completo centrado en los riesgos de esta tecnología. En lo que se refiere al coche autónomo, el Libro Blanco establecía que el humano debe poder interferir en la máquina para detener su funcionamiento. Ve positivo promover el monitoreo del sistema de inteligencia artificial mientras el AV está en funcionamiento y la capacidad de intervenir en tiempo real y desactivarla.

Para entender los cambios legislativos que supondrá el coche autónomo basta con ver la legislación y sentencias que ha generado la introducción en el último lustro de los patinetes eléctricos en los viales y obligó al Gobierno de España a definirlos como vehículos. Una sentencia del 13 de noviembre del 2019 dictada por el Juzgado de lo Contencioso-Administrativo número 3 de Alicante señala que «desde el ámbito de la legislación de tráfico los dispositivos de movilidad personal tendrán la consideración de vehículos, de conformidad con la definición que al efecto establece el Anexo I del Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial (TRLSV)». Eso incluye una definición de responsabilidades civiles y penales de fabricantes, conductores y peatones en caso de accidentes. Prevén que tanto la abogacía como el sector asegurador tendrán que hacer una revisión obligatoria de la legislación actual en materia vial. El CGAE admite que la tecnología del coche autónomo se desarrolla más lenta de lo esperado y confía en que en los próximos años continúe desarrollándose el marco legal y legislativo que impulse estos vehículos, preparando el terreno para cuando se disponga de la tecnología necesaria.

Actualmente, la legislación respecto al coche autónomo está avanzando en los países que regulan esta rama de la IA. En Estados Unidos y el Reino Unido, la normativa se centra en la aprobación y regulación de las pruebas y test de prototipos en las carreteras, donde ya ha habido atropellos mortales con estos vehículos autopilotados y en prohibir los *spy cars* (coches espía) y los ataques cibernéticos. En la UE, cualquier regulación de los coches autónomos debería cumplir los siete requisitos esenciales expuestos en el Libro Blanco de la Inteligencia Artificial de la UE que son los de acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y de los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y medioambiental y rendición de cuentas. La UE

advierte que alguna de estas directrices del grupo de expertos de alto nivel, que no son vinculantes, como la transparencia, el seguimiento y la supervisión humana, no son contempladas de manera específica en la legislación en vigor de numerosos sectores económicos. Pero en todo caso, cree que un marco regulador claro que las recogiese generaría «confianza» entre los consumidores y las empresas.

Los legisladores están optando por adaptar la legislación vigente como el Convenio de Viena de 1968 para la circulación del tráfico automatizado. En la UE ya han surgido iniciativas como la Directiva 2010/40/EU del Parlamento Europeo del 7 de Julio de 2010 en el marco del desarrollo de Sistemas de Transporte Inteligente en el campo del transporte de carretera y para las interfaces con otros modos de transporte. Por su parte, el Departamento de Transporte del Reino Unido elaboró en julio del 2015 la guía The Pathway to Driverless Cars: A Code of Practice for Testing y en el 2018 la Automated and Electric Vehicles Act. Y, por su parte, el Congreso de Estados Unidos ha publicado en 2016 y 2017 dos memorandos, uno respecto a los AVs y sus niveles de automatización para proteger al consumidor, y otro sobre el futuro de estos coches autopilotados. La nueva Automated Vehicles (AV) Bill, el nuevo marco de seguridad anunciado por el Parlamento del Reino Unido el 7 de noviembre de 2023, pretende garantizar una responsabilidad clara para el usuario, establecer el umbral de seguridad para la conducción autónoma legal y establecer un esquema regulatorio en uso para monitorear la seguridad continua de estos vehículos.

Varios países, como Bélgica o el Reino Unido, han establecido protocolos como una respuesta práctica para acomodar las pruebas y test de AVs en los viales convencionales y garantizar la responsabilidad en cuanto a la seguridad de otros usuarios. Estas pruebas suelen requerir la presencia de un conductor humano, aunque el vehículo circule en modo automático. En las áreas peatonales, debe hacer un mínimo de distancia para que el operador pueda aplicar la parada de emergencia desde fuera del vehículo. Deben tener una toma del control rápida si fuese necesario y tener niveles apropiados de seguridad ante riesgos de jaqueo informático. También se les exige una «caja negra» de datos grabados para analizar en caso de un incidente. Este tipo de códigos de prácticas exigen que el coche automático vaya asegurado en las pruebas.

El británico BANZI estudia aspectos como la definición de «conductor» (driver), el problema del tranvía y las soluciones legislativas y diversas cuestiones sobre el «Social Dilemma» (dilema social) y los códigos éticos que deben usar los ingenieros de software robótico. GLASSBROOK estudia los problemas legales generados por estos vehículos y las futuras leyes que se pueden aplicar a los coches guiados por IA. Cameron propone reformas legales como la responsabilidad criminal, la regulación del *testing*, la ciberseguridad, el mandato de conectividad, el uso de espectro de radio, la planificación urbana, el uso de carriles especiales o el aparcamiento, así como la ética y la privacidad. CHANNON y otros identifican las «áreas grises» y las lagunas de la ley actual, no solo en el Reino Unido, sino también en Alemania, Italia, Austria, Grecia o Sudáfrica. Hace especial alusión a la Convención de Viena de Tráfico de 1968 o la Regulación ECE número 79.02 del 2017 de la

ONU. Admite que los vehículos «quasi-autónomos» ya están aquí, rodando tanto en pruebas privadas como comerciales. Está de acuerdo en que la legislación británica y otras ya están implementado reformas legales como la *Automated And Electric Vehicles Act* de 2018, centrada en los seguros de tales coches y aplicando cambios a la *Road Vehicle (Construction And Use) Regulations* de 1986 y el código de autopistas.

4. Ciberseguridad

El Gobierno británico también ha lanzado una guía no-estatutaria respecto al chequeo de las carreteras públicas y la relación de estos vehículos con la ciberseguridad. En el Congreso de Estados Unidos un senador llegó a plantear en el 2019 el proyecto de ley *SPY Car Act* que imponía la obligación de que el coche autónomo detectase y reportase los ciberataques o intentos de toma de control y protegiese los datos almacenados por el coche tanto estacionado como en movimiento. Aunque se introdujo en el Congreso, la *SPY Car Act* no se convirtió en ley, pero revela el interés de los senadores por prevenir otro de los grandes problemas de los AVs. CHANNON cita en EE.UU., varias leyes publicadas al respecto como la *Advancement of Revolutionary Technologies Act 2017* (AV START Act) del 2017 o la *Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act 2017* (SELF DRIVE Act). Posteriormente, en el 2024, Estados Unidos barajó por cuestiones de seguridad nacional prohibir los coches eléctricos chinos BYD por riesgo de que sus sensores los convirtiesen en *spy-cars* para una potencia extranjera. CHANNON añade la protección de datos y el chequeo de las carreteras. Aborda el concepto de «responsabilidad vicaria» cuando una persona debería ser responsable de los actos de otra muy estrechamente conectada. Todo hace pensar que se trata de un instrumento del Derecho muy útil para atribuir responsabilidades en los AVs.

La ciberseguridad de los AVs ha sido puesta de relieve por la canadiense Herdman la cual se pregunta cómo toman sus decisiones los vehículos autónomos e indaga en los fallos actuales del software. Avisa de los «negativos efectos que el software puede tener en nuestras vidas» y los riesgos que supondrá el salto del coche en el siglo XXI, cuando los robot-cars empiecen a circular por las carreteras. La autora sospecha que si esto no se ha regulado aún es porque los legisladores creen en la «magia» de la tecnología que hace milagros y lamenta las escasas iniciativas a este respecto emprendidas por la *National Highway Traffic Safety Administration* (NHTSA) de Estados Unidos. Por el contrario, SMITH cree que las diferentes legislaciones internacionales, como las de la *Federal Motor Vehicle Safety Standars* o el Convenio de Viena de 1968, no prohíben categóricamente la legalidad de los coches autónomos. Se basa en aspectos como el control indirecto del vehículo. NOGUÉRO (2019) y TAEIHAGH y LIM han asumido la tesis de la *Society of Automotive Engineers* (SAE) de clasificar a los AVs en cinco niveles de conducción autónoma o semiautónoma, así como varios grados de responsabilidad civil, incluso la pluralidad de responsables o la responsabilidad en cascada. Habrá que dirimir si el daño procede del programador, del fabricante o del usuario en los accidentes provocados por estos vehículos robotizados. Al ir

dotados con sensores y ordenadores a bordo que pueden sufrir averías o mal mantenimiento, la responsabilidad se extiende al conductor.

Una solución que ve el Reino Unido para limitar los accidentes es construir vías especiales (dotadas de sensores y comunicación entre vehículos y con las señales de la carretera, sin cruces, o sin interacción con los peatones) para que los vehículos automáticos circulen con total seguridad. Pero esa no parece ser la estrategia a seguir ni por los poderes públicos ni por las compañías fabricantes, a excepción de los ensayos que se puedan realizar algunos campus universitarios, los proyectos reducidos a entornos cerrados o las llamadas *smart cities* (ciudades inteligentes). Cabe mencionar el caso de China, donde desde el 2018 se han habilitado circuitos de pruebas en entornos reales. Todo apunta a que los gobiernos tendrán que adaptar la legislación de seguridad vial a un mundo real donde los coches autónomos y conductores humanos compartirán la vía pública con los riesgos que eso conlleva. Como señala LIPSON, ningún gobierno va a invertir en construir autopistas inteligentes hasta que no haya coches inteligentes y una comunicación V2X (comunicaciones de vehículo a vehículo y de vehículo a infraestructura). El informe España Digital 2025 prevé que el 5G tendrá gran impacto en la automoción. La regulación de los coches autónomos va ligada también al desarrollo de las *smart-cities* y de dichos corredores, algo que contempla la comunicación de la Comisión Europea «La conectividad para un mercado único digital competitiva–hacia una sociedad europea del Gigabit».

II. LOS DILEMAS ÉTICOS DE LA PROGRAMACIÓN DE ALGORITMOS

La controversia sobre los AVs genera discusiones éticas, muchas de ellas versiones del «dilema del tranvía», un experimento mental ideado por FOOT. Un tranvía se sale de control y en su camino hay cinco personas atadas a la vía por un filósofo malvado. El conductor debe decidir si acciona un botón para desviarlo a otra vía, donde hay otra persona atada. La mayoría de los consultados acciona el botón para salvar cinco vidas a cambio de sacrificar una. No hacer nada ocasionaría mayores pérdidas humanas. Hay más versiones del dilema expuestas por THOMSON y UNGER. Pero las marcas de fabricantes de automóviles hicieron su propia consulta a los consumidores para conocer la solución que prefieren a estos dilemas éticos y los encuestados responden mayoritariamente que no comprarían un coche autónomo que no salvase la vida de su dueño. Quieren coches egoístas.

En el caso de la UE, hay un amplio conjunto de derechos sustantivos de los consumidores que los protegen y empoderan al realizar actividades económicas en el mercado único, que incluye los derechos de devolución de un productor, de exigir que se repare o sustituya un producto defectuoso dentro de su período de garantía. A mayores existen un conjunto de instrumentos de la UE para la garantía del cumplimiento y un abanico de resoluciones alternativas de litigios en materia de consumo (RAL) mediante mecanismos extrajudiciales.

Para comprender la complejidad de los problemas legales que puedan generar los coches sin conductor hay que contextualizar los conflictos resultantes dentro de una economía digital altamente compleja que numerosos teóricos estudian a partir de la segunda década del siglo XXI. A los problemas éticos emanados del dilema del tranvía o la paradoja de Collingridge (1980), se suman otros relacionados con la extracción de datos de las rutas de los conductores para alimentar los algoritmos de las plataformas que actualizan el software de los vehículos autopilotados. En este contexto, las redes inalámbricas 5G y la IoT son clave para los coches autónomos porque estos pueden responder a un estímulo en tiempo real (latencia baja) y, además, permiten una enorme recolección de datos de la conducción y las rutas. Aquí se incluyen los debates éticos (los llamados Ethics 2.0), que giran en torno a las decisiones tomadas por la IA y al funcionamiento de la Internet de las Cosas (IoT), los entresijos de la denominada «era del capitalismo de vigilancia» descrita por Zuboff, Shoshana. o la proposición de nuevas leyes de la robótica. En es en este contexto en el que se podría encuadrar la responsabilidad civil en casos con vehículos autónomos.

Para BONNEFON los vehículos autónomos deberían reducir los accidentes de tráfico, pero en ocasiones tendrán que elegir entre dos males, como atropellar a los peatones o sacrificarse a sí mismos y a su pasajero para salvar a los viandantes. Definir los algoritmos que ayudarán a los AVs a tomar estas decisiones morales es un «desafío formidable», según este autor. El filósofo LIN junto con JENKINS y ABNEY plantean diversos dilemas éticos 2.0. generados por los robots, lo que incluye los coches autónomos. BHARGAVA insiste en que estos coches estarán lastrados por la incertidumbre al actuar cuando la persona con la autoridad para elegir la ética del vehículo se encuentra bajo una incertidumbre moral (tiene acceso a hechos no morales relevantes como los empíricos y legales pero aún permanece inseguro acerca de lo que la moralidad requiere de él). Pretende lograr soluciones inspirado en el filósofo SEPIELLI. BANZI plantea lo que denomina un «dilema social» respecto a los coches autopilotados, los AVs. Se refiere a que esas encuestas en las que los consumidores prefieren que el vehículo autónomo tome una decisión «utilitaria» y ética.

Respecto a dichas propuestas, COCA VILA se muestra contrario a las soluciones utilitarias y advierte que, en el marco de un sistema legal liberal que reconoce a los humanos como agentes libres que tienen derechos y responsabilidades, maximizar la función de utilidad social no justifica una injerencia perjudicial en la esfera jurídica de una persona.

En sentido estricto, BANZI propone un código ético de conducta elaborado por un consejo o comisión denominado *Robotics and Autonomous Systems Leadership Council* (RASLC) para analizar los sistemas autónomos en un marco ético transparente y así coordinar los sectores de la automoción antes de llegar al coche totalmente autónomo. Aduce los riesgos directos para la salud y en potencia altamente letales de los sistemas autónomos. Propone un código ético de conducta válido para soportar las responsabilidades por negligencia profesional por defecto en los AVs.

En la práctica, una de las estrategias efectivas ha sido exigir más test a los fabricantes y desarrollar los llamados crash algorithms (algoritmos de colisión), que predicen todos los escenarios posibles de accidentes inevitables y establecen al AV cómo reaccionar. Seguir haciendo pruebas y ensayos, es la solución provisional adoptada por algunos legisladores ante la dificultad de resolver el dilema ético del tranvía y reconciliarlo con el egoísmo del conductor de los AVs.

En cuanto a TAIEHGAH y LIM, siguiendo a COCA VILA sospechan que los algoritmos van a ser programados para salvar a los ocupantes del coche sobre todo lo demás, lo que le confiere viabilidad económica al fabricante. Coca Vila propone como solución penalista que los coches autopilotados dispongan de una «moral de excepción» preestablecida a través de algoritmos que regulen su modo de operar en situaciones de necesidad, como por ejemplo, disponer de patrones de conducta en escenarios en las que la salvaguarda de un concreto interés exija irremediablemente la lesión de otro. El conductor tiene la posición de *dominus*.

Conviene recordar que los algoritmos con los que navega un coche están protegidos en Estados Unidos por la ley de secretos empresariales (y no de patentes) como es el caso de la *Defend Trade Secrets Act of 2016*. Para PASQUALE las empresas tecnológicas han conseguido dotarse de un marco jurídico más favorable a sus intereses. Dice que el *trade secrecy protection* crea efectivamente un derecho de propiedad sobre un algoritmo sin requerir que sea revelado. Si sale a la luz, pierde su protección legal.

En España, los secretos empresariales están regulados por la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que, siguiendo a HUERGO LORA traspone la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. El secreto empresarial, al contrario que la patente registrada, no tiene límite temporal. Todo esto tiene transcendencia para el usuario que intente probar la negligencia o culpa de una plataforma o un fabricante en un accidente con AVs.

III. LA ACT AI Y LA RESPONSABILIDAD DEL COCHE AUTÓNOMO

La puesta en marcha del coche autónomo estuvo pendiente de la aprobación del texto definitivo de la *AI Act* (AIA), aprobado por el Consejo de la UE el 21 de mayo de 2024 y con entrada en vigor en el 2026, o antes, parcialmente. El texto no cita expresamente la IA de los coches autónomos, lo que resulta decepcionante respecto a la importancia que podría adquirir en un futuro pero se sobreentiende que forma parte de aquellos productos o componentes de IA que pueden provocar un "incidente grave", definido como un incidente o un mal funcionamiento de un sistema de IA que provoque directa o indirectamente, entre otras cosas, la muerte de una persona o un daño grave para la salud de una persona. Aplicando la *AI Act*, se les podría encuadrar como máquinas de alto riesgo. Por otra parte, los sistemas de

seguridad de los coches autónomos avanzados están regulados en el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo.

1. La IA como componente de un producto

La IA podría entenderse como una unidad técnica independiente destinada al vehículo. Autores como ATIENZA NAVARRO dudan de que los programas de IA sean un «producto» aunque, desde nuestro punto de vista, no pueden ser sino eso mismo ya que son manufacturas electrónicas. Dicho reglamento de seguridad del 2019 prohíbe a los sistemas de la IA del coche autónomo extraer los datos biométricos de los usuarios (prohibido ya en la *AI Act*, salvo excepciones) pero hay un caballo de Troya en cada vehículo: el teléfono móvil del conductor o el pasajero, el cual pronto llevará instaladas apps de IA que, previsiblemente, registrar todos los movimientos del usuario en el vehículo. Por otra parte, el apartado 11 del mismo reglamento prevé un deber de disponer de la posibilidad de desactivar el asistente de velocidad inteligente, por ejemplo, cuando el conductor reciba falsas advertencias o información inadecuada de viales o señalización. La función de desactivación quedará bajo control del conductor. Y no hay que olvidar que el apartado 2 del Anexo III de la *AI Act* (que remite al apartado 2 del artículo 6) considera que la IA usada en infraestructuras críticas, como el transporte, es de alto riesgo porque podría poner en peligro la vida y salud de los ciudadanos. Esto obliga a implantar a la industria del automóvil sistemas adecuados de evaluación y mitigación de riesgos, que estos productos sean de alta calidad, que haya trazabilidad y otras medidas de seguridad.

Según la definición 14 del artículo 3 de la Ley de la IA, los sistemas de IA que son componentes de seguridad de productos (caso de la IA de un robot cirujano) son un componente de un producto o de un sistema de IA que cumple una función de seguridad para dicho producto o sistema de IA, o cuyo fallo o mal funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes. También la IA es considerada como productos en sí mismos, y entran dentro del ámbito de aplicación de determinada legislación de armonización de la Unión, y procede considerarlos de alto riesgo si el producto en cuestión es sometido al procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad externo de acuerdo con dicha legislación de armonización pertinente de la Unión. El párrafo 31, señala que para que un sistema de IA se considere de alto riesgo no significa necesariamente que el producto del que sea componente de seguridad, o el sistema de IA en sí mismo como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la legislación de armonización de la Unión pertinente que se aplique al producto.

El considerando 55 de la *Act AI* alude al tráfico rodado o por carretera en los que los sistemas de IA están destinados a ser utilizados como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas y el tráfico rodado, así como el suministro de agua, gas, calefacción y electricidad, pues su fallo o defecto de funcionamiento puede poner en peligro la vida y la salud de las personas a gran escala y provocar perturbaciones apreciables en el desarrollo ordinario de las actividades sociales y económicas. Varios apartados sucesivos de la *AI Act* hacen alusión al entrenamiento de modelos de la IA y a la ciberseguridad, que también pueden afectar a los vehículos autónomos, al entenderse que son máquinas de alto riesgo, lo que exige que sean supervisados eficazmente por personas físicas (artículo 14.1 de la *AI Act* sobre supervisión humana). Hay obligación en los sistemas de alto riesgo de registrar los datos generados automáticamente (artículo 12 de la AI Act) y que parece evidente que afecta al coche autónomo durante su vida útil del sistema y expresamente para los eventos relevantes. Eso obligaría a dotar a dichos vehículos de una "caja negra" que registre toda su actividad.

El artículo 25 de la *AI Act* atribuye expresamente la responsabilidad al fabricante (que será el responsable de que el sistema de IA de que se trate cumpla lo dispuesto en el reglamento) porque forma parte de la cadena de valor de la IA. Ateniendo a las disposiciones del texto provisional del reglamento o de la *AI Act* se pueden examinar las distintas interacciones entre los actores que conforman el ecosistema de la IA, aplicado al coche autónomo, y por la que se podrían generan acciones jurídicas o de las que emanen responsabilidades, en la mayoría de los casos de tipo civil, pero sin excluir las consecuencias penales. No hay que olvidar que un automóvil autónomo es una máquina o un robot de alto riesgo y cuyas decisiones, basadas en cálculos y predicciones, pueden generar graves riesgos para otros usuarios de la vía.

2. La dificultad de cumplir la exigencia de la trazabilidad

En cuanto a las plataformas que desarrollan los coches autónomos, estas podrían incurrir en diversos tipos de responsabilidad. Una de sus características negativas es que actúan con opacidad amparadas en la ley de secretos industriales y patentes, como ya se explicó, a lo que se suma que el diseño de una IA entrenada con aprendizaje profundo se basa en cajas negras o *black box* y, realmente, por razones técnicas, a día de hoy, es altamente improbable que se logre la trazabilidad que exige la *AI Act* a los productos de alto riesgo (artículo 12, considerandos 27 y 53, y anexo VIII). A efectos prácticos, estas máquinas siguen un razonamiento no-humano, cuyo resultado se basa en el análisis de miles o millones de variables o parámetros, y son incomprensibles para los humanos. Esto supone un importante obstáculo a la hora de que la víctima de un accidente intente probar la responsabilidad de una plataforma, un programador o un fabricante porque no hay una trazabilidad que localice el fallo que propició el siniestro vial, a no ser que sea muy evidente. Podría tratarse de una línea de código errónea o un parámetro pasado por alto entre millones de líneas de código.

En cuanto a la trazabilidad, transparencia y la privacidad de la IA, la propuesta de la *AI Act* ya las protegía expresamente en el considerando 9 bis, redactado de nuevo tras una enmienda de junio del 2023. y que reza así: «(9 bis) Es importante señalar que los sistemas de IA deben hacer todo lo posible para respetar los principios generales que establecen un marco de alto nivel que promueva un enfoque coherente centrado en el ser humano con respecto a una IA ética y fiable, en consonancia con la Carta de los Derechos Fundamentales de la Unión Europea y los valores en los que se fundamenta la Unión, como la protección de los derechos fundamentales, la intervención y vigilancia humanas, la solidez técnica y la seguridad, la privacidad y la gobernanza de datos, la transparencia, la no discriminación y la equidad y el bienestar social y medioambiental». El considerando 9 bis es aplicable al resto del presente análisis, pero también el 14, que incide en la obligación de la transparencia de la IA. Una solución posible sería la instalación de cajas negras en los vehículos autónomos (garantizando la privacidad para evitar que la caja negra tenga la doble función de explotar los datos del conductor).

3. Responsabilidad de las plataformas, el fabricante y el desarrollador

Otra parte de la responsabilidad recae en la plataforma a la hora de definir sus estrategias, que al ser empresas de lucro se basan en la obtención del mayor beneficio posible. Esto propicia una lógica que apuesta por aplicar tácticas monopolísticas para adueñarse del ecosistema que rodea al coche autónomo para tener una posición dominante en el mercado. Las plataformas, probablemente, no puedan controlar el negocio de las materias primas (litio para las baterías, hierro y aluminio) pero sí están en disposición de mantener su dominio en el negocio de los datos y la IA (sistemas GPS y de navegación autónoma, telecomunicaciones, redes sociales, granjas de servidores y centros de datos), la distribución de energía (surtidores eléctricos) y el diseño e ingeniería de la fabricación (la marca). Lo ideal, para una plataforma, es que el usuario compre la electricidad de su vehículo autónomo en los surtidores propiedad del mismo grupo, conduzca un coche de la misma marca y proporcione datos de sus rutas a la Nube de la misma compañía, la cual usará para entrenar a su modelo de IA o para reexportar a terceros. Las políticas antimonopolio de la UE para la vigilancia del mercado les perjudican porque les obligarían, en un futuro, probablemente, a trocear su negocio con estructura vertical.

En cuanto al programador informático, su responsabilidad consiste, además de poner en marcha un algoritmo funcional y seguro, en evitar que su diseño del algoritmo genere sesgos o discriminaciones que perjudiquen a otros usuarios de la vía, obligación ya vista en el mencionado considerando 9 bis de la *AI Act*. Algunas propuestas de expertos sugieren que los ingenieros, matemáticos y programadores que trabajan en la generación de algoritmos realicen un juramento hipocrático para comprometerse a no hacer daño o guiarse por unos protocolos éticos o negarse a realizar un trabajo que contradiga su código deontológico (a fin de justificar una indemnización en caso de ser despedidos por motivos disciplinarios). Algunas empresas ya están aplicando unos protocolos éticos para limpiar de sesgos y discriminaciones sus algoritmos. Una de sus obligaciones sería facilitar la trazabilidad del

vehículo, en consonancia con el nuevo artículo 9 bis de la *AI Act*, para ayudar a los investigadores de accidentes de tráfico a localizar el origen del fallo en el programa que generó una decisión errónea del AV.

La principal responsabilidad del programador es evitar que él incurra en una negligencia o descuido. Debe suprimir o prever cualquier fallo de programación de los algoritmos que generen accidentes cuando el vehículo autónomo ruede por la carretera, pues lo contrario podría considerarse un producto defectuoso (el Libro Blanco de la UA sobre la IA considera que esa es una línea a seguir). Una de sus obligaciones es someter a un exhaustivo entrenamiento al algoritmo para que pueda actuar en todas las situaciones posibles (decisiones en árbol). Muchas veces se recurre a un ejército de trabajadores fantasma para entrenar al algoritmo o a los propios usuarios (aquel ejercicio de probar que el usuario no es un robot mediante el reconocimiento e identificación de distintos tipos de semáforos en una serie de imágenes). Sin embargo, muchos de estos entrenamientos están automatizados (la máquina entrena contra sí misma o se nutre de datos extraídos de los usuarios) y, además, estos sistemas se retroalimentan mediante aprendizaje profundo (analizando millones de rutas de los usuarios para establecer el itinerario más corto y seguro). La propia opacidad de las plataformas impide localizar el origen de los fallos del algoritmo o probar que la IA se basó en datos erróneos, puesto que, como ya se comentó, el sistema de IA de conducción autónoma es un secreto industrial protegido. Y hay que tener en cuenta que una máquina de este tipo toma decisiones no supervisadas por humanos. Dado que la responsabilidad no puede recaer en una máquina, aunque se intentó introducir la fórmula de la personalidad jurídica, habría que buscar a un responsable humano y la UE apunta a la figura del implementador.

Es más fácil la detección de un fallo de seguridad (o bug) que se hace evidente cuando un jáquer o un malware aprovecha las vulnerabilidades del programa de IA para «secuestrar» un coche autónomo. Exige una inversión previa en ciberseguridad para proteger un algoritmo que usarán millones de usuarios en situaciones de riesgo en la carretera. Esta preocupación por la falta de inversión en ciberseguridad la compartía ya la enmienda 17 de la Propuesta de Reglamento de la *AI Act* en el Considerando 5 bis (nuevo). Esos *bugs* o lagunas podrían eliminarse si la compañía premia a cazarrecompensas o convoca torneos o juegos de equipo rojo y azul que detecten los agujeros antes de que la versión final del programa salga al mercado. Como el sistema opera con una IA, sería conveniente hacer ataques previos con una IA adversaria, o dos IA contrapuestas o antagonistas.

La responsabilidad del fabricante del coche es más evidente que la del programador, puesto que mientras que es difícil probar un fallo o error del algoritmo que controla un automóvil, los investigadores de accidentes o daños están más familiarizados con las averías de los vehículos de conducción humana. La peculiaridad del coche autónomo es que este tiene tres componentes novedosos: es eléctrico (el enchufe puede cargar mal), funciona con baterías (pueden ser defectuosas e incendiarse), usa cámaras dotadas de reconocimiento de imágenes, antenas receptoras de 5G y sensores (susceptibles de averiarse y deben

reemplazarse) y llevan pantallas y ordenadores de a bordo. Estos fallos son fáciles de detectar (por ejemplo, que se estropee una cámara o un sensor y el algoritmo quede «ciego» y no pueda leer una señal de Stop en la carretera), y se podía aplicar la legislación sobre productos defectuosos y reclamar indemnizaciones por la vía civil. El fabricante sería responsable si la avería estuviese cubierta por la garantía de la marca. Hay otros factores medioambientales, como la temperatura, que podrían sobrecalentar el vehículo y sus dispositivos internos, que generarían más controversia sobre quién debe recaer la responsabilidad. La cuestión que se plantea es hasta qué punto la responsabilidad recae en el fabricante cuando falla el algoritmo porque, por ejemplo, no está bien entrenado por el programador. ATIENZA NAVARRO considera que los fallos de software han de considerarse también como defectos de diseño pero, en todo caso, equipara al proveedor de software, al de hardware, y al de infraestructura como sujetos incluidos en el término de productor según la reforma de la Directiva 85/374/CEE. Al no haber una trazabilidad (que sí es exigida en la *AI Act*), no se puede probar. Y el coche autónomo es una máquina que está tomando continuamente decisiones protegidas por la opacidad. Una solución sería establecer una cadena o cascada de responsabilidades entre los integrantes de la puesta en marcha de un AV, que incluye la fabricación, la programación y entrenamiento del algoritmo y la estrategia empresarial.

Al analizar la responsabilidad del usuario, hay que distinguir entre coches autónomos de nivel 5 (robotaxis, que ya están operativos en China y California) y coches en los que el ser humano tiene algún tipo de intervención o supervisión. Cuando hay supervisión humana, la responsabilidad recae en este por no estar atento a la carretera, tomar el control e intervenir ante la situación de riesgo o anuncio de peligro. Hay jurisprudencia que condena a un usuario que supervisaba la conducción autónoma en un test de entrenamiento y, por no estar atento a la vía porque veía un vídeo, atropelló a un ciclista que la máquina tardó en reconocer. ATIENZA NAVARRO propone que la responsabilidad incida más en el propietario del vehículo que en el usuario porque los coches autónomos pueden ser vehículos compartidos. En este sentido, el propietario del vehículo-robot puede tener responsabilidad en un accidente respecto al mantenimiento del vehículo si no ha cumplido con su obligación de supervisar el estado de las ruedas y comprobar que no estaban defectuosas, o reemplazar una cámara con un visor roto o los sensores averiados antes de regresar a la vía. La misma responsabilidad podría atribuirse a los operarios de mantenimiento que hicieron un servicio y cometieron una negligencia profesional (instalar una pieza defectuosa). El usuario también puede ser el pasajero y a él cabe atribuir responsabilidad por comportamiento temerario dentro del vehículo compartido o por generar distracción al conductor cuando este toma el mando del vehículo. El no estar atentos a la vía cuando la conducción es parcialmente autónoma puede generar consecuencias jurídicas para el infractor, así como provocar maniobras temerarias.

4. La Nube como tecnología crítica de alto riesgo

La Nube o *Cloud*, que podría considerarse como una infraestructura digital crítica cuyos fallos pueden producir eventos graves, generará situaciones de responsabilidad para su propietario, que es la plataforma. Aquí se incluyan los fallos de navegación de GPS, errores

en el mapa de tráfico, caídas del sistema de IA o de la comunicación entre sensores y los servidores, que se pueden considerar averías que han propiciado un «apagón» en el coche autónomo y el consiguiente accidente de tráfico, que puede dañar a terceros. Pero la Nube también genera otro tipo de responsabilidad que consiste en la extracción no consentida de datos del usuario al elaborar patrones con sus itinerarios y que podría suponer una vulneración a los derechos de privacidad o intimidad del usuario, proscritas por el considerando 9 bis de la propuesta de *AI Act* y por otras enmiendas aprobadas en junio del 2023. Para guardarse las espaldas, la plataforma podría hacer firmar un contrato de aceptación de condiciones de uso para obligar al usuario a ceder la propiedad de las imágenes que graben las cámaras en el exterior. Pero, a mayores, elaboraría patrones sobre los hábitos del conductor que permitirían deducir sus rutinas diarias y las excepciones o irregularidades de ciertos días de la semana, su estrato económico o su ideología (si aparca muchas veces en una iglesia de determinada confesión o en la sede de un sindicato). La industria extractiva de datos (el llamado «capitalismo de vigilancia» que describió ZUBOFF) no se limita a acumular información sobre el usuario sino también en influir en su comportamiento para que dedique más tiempo de su atención a productos que le interesan a la plataforma, a orientar o cambiar su voto o a otros motivos que benefician a terceros, todo ello sin el conocimiento del usuario. Una industria extractiva de datos intenta captar el máximo de atención del usuario, y el coche es un nuevo espacio a «colonizar». Esta influencia en el comportamiento podría llegar, teóricamente, a casos extremos en los que el algoritmo traza rutas, de forma levemente alteradas, que pasan por delante o que buscan plaza de aparcamiento ante determinados establecimientos comerciales que son clientes de la plataforma a fin de animar al usuario a hacer una parada. Hay otro tipo de responsabilidades que son más fáciles de determinar y que se refieren a las infraestructuras de las carreteras. Del Estado y de las operadoras de telefonía cabe exigir otra responsabilidad, que es el correcto mantenimiento de la red de antenas de 5G o la futura 6G y de la total cobertura de la transmisión en los viales.

La plataforma está sujeta a diversas leyes o proyectos legislativos dictados en la UE que regulan los productos defectuosos (Libro Blanco de la UE) o el nivel de riesgos de sus productos (la *Act AI*, que entrará en vigor en 2024 o sucesivos). Su actividad también está sujeta a la Ley de Servicios Digitales (LSD) para proteger a los consumidores y sus derechos fundamentales en línea, establecer unas líneas de transparencia y reducir los contenidos ilícitos. La LSD hace especial mención a la categoría de plataformas en línea de muy gran tamaño porque plantean especiales riesgos en cuanto a difusión de contenidos ilícitos y nocivos para la sociedad, y que les puede obligar a estar supervisadas por la Administración. Del mismo modo, las grandes plataformas deben cumplir las normas europeas de monopolio y de libre competencia si quieren operar en ese mercado. En Estados Unidos, están sometidos a las leyes *AntiTrust*. Sin embargo, como ya se comentó, las plataformas están amparadas por la Ley de Secretos Industriales de EE.UU., su funcionamiento sigue estando blindado y le permite operar con opacidad, lo que dificulta obtener la prueba.

Mientras la LSD ampara a los consumidores, la RGPD protege a los usuarios de la invasión de la privacidad y de la extracción de datos no consentida. Los coches autónomos van a enviar datos de los usuarios para mejorar las rutas o actualizar la visión general del tráfico pero, a la vez, son entrenadores de la IA cada vez que viajan, y miles o millones de parámetros son analizados y empaquetados para su reventa.

En cuanto al diseñador y programador del algoritmo, este ha de cumplir con la legislación sobre derechos fundamentales del ser humano (no discriminación, dignidad) para evitar sesgos que perjudiquen al usuario cuando este contrata un seguro o aspira a un trabajo. Dado que la mayoría de los programadores son asalariados que deben cumplir con unos objetivos, proyectos o estrategias de sus empresas, hay una propuesta para que se acojan a un código deontológico o juramento hipocrático para informáticos en caso de que consideren que se han vulnerado ciertas normas éticas. Ciertas consultoras como McKensey permiten a sus empleados rechazar proyectos si van contra su conciencia (asesorar a una tabaquera o una extractora de combustibles fósiles). Numerosos países están suscribiendo los principios éticos de la IA de la UNESCO, y organizaciones y foros empresariales (OCDE, Foro de Davos, WEF) fomentan su propia autorregulación ética.

Más grave es la responsabilidad civil del programador cuando un error de código genera accidentes, lo que convierte al coche autónomo y a su algoritmo de la IA en un producto defectuoso. En ese caso, habría que aplicar los postulados del Libro Blanco de la Inteligencia Artificial de la IA. El programador y el director de producto (*product manager*) son dos eslabones de la cadena de responsabilidades en cascada de la producción de un coche autónomo defectuoso pero para el usuario o la víctima del accidente será difícil probar dónde está el error, incluso si se encargan informes forenses, debido a la opacidad y el secreto industrial, algo que ya ha previsto la UE en una regulación accesoria en la que suaviza los requisitos para que un consumidor pruebe las causas.

En cuanto al fabricante, este es el responsable directo de que un coche autónomo resulte ser un coche defectuoso y, en lo que respecta a la IA, estar sujeto a las propuestas del Libro Blanco de la UE. Conviene distinguir entre un fallo en el hardware (la carrocería, las baterías, los sensores, la antena) y el software (algoritmo de navegación). En ese caso, puede resultar que el fabricante del algoritmo es una plataforma distinta de la compañía que manufacturó el vehículo. Pero ambas suelen estar fusionadas, por ejemplo, en el caso de Tesla (que fabrica coches y les instala su propio software de IA y los servicios asociados que surgirán a medida que aumente el nivel de automatismo). El fabricante también está sujeto a otras legislaciones como la medioambiental. No se está penalizando en la regulación el alto consumo energético generado por la minería de datos.

En el caso de que el siniestro vial se debiese a un fallo del algoritmo de nivel 5 sin intervención del usuario (el coche bruscamente cambia su rumbo y empieza a correr alocadamente hacia un grupo de peatones a los que arrolla; las llamadas «alucinaciones» de la IA), habría que pedir responsabilidades al fabricante o a la plataforma (por motivos legales, seguramente estarán disociados) pero no al usuario. Si este es un supervisor de la conducción

autónoma o toma el control en determinados tramos, la responsabilidad civil o incluso penal podrían recaer sobre él por despiste, no atención a la carretera o falta de reacción, entre otros.

A nivel penal, hay algunas posibilidades como que el usuario use el coche autónomo como un arma homicida. Por ejemplo, el usuario reprograma el código para que el vehículo ignore a los peatones en un determinado tramo de la carretera y atropelle a su objetivo a la que hora que siempre pasa. Es una posibilidad teórica pero, probablemente, estos vehículos se podrán manipular por ejemplo, como herramienta para transportar drogas o contrabando sin riesgo para el traficante.

En el caso de la Nube o *Cloud* que dirige la navegación del vehículo autónomo mediante un sistema de IA, además de que sea un producto defectuoso (y oriente mal al vehículo de forma que le ocasione un accidente), está sujeto también a las regulaciones que deriven del Libro Blanco de la UE y la *AI Act*. Pero lo más preocupante es la extracción de datos del usuario dentro de la lógica de la economía de la atención o de otro tipo. En ese supuesto, se podría aplicar la RGDP, por invasión de la intimidad. Y la *Act AI* penaliza la manipulación del comportamiento del usuario.

IV. CONCLUSIONES

La *AI Act* aprobada por el Consejo de la UE el 21 de mayo de 2024, apoyada por el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 sobre seguridad en los vehículos a motor (incluidos los autónomos) despliegan un amplio arsenal de preceptos que obligan a las empresas que implantan productos dotados de inteligencia artificial a cumplir derechos fundamentales relacionados con la privacidad, la transparencia, o la no discriminación, así como la obligación de invertir en ciberseguridad. Estas disposiciones serán muy útiles para proteger la intimidad del consumidor a medida que se implante el coche autónomo y este se convierta en un producto habitual en las carreteras, una infraestructura crítica. La razón es que el coche autónomo está concebido, desde el punto de vista de las plataformas digitales, como un dispositivo multimedia de extracción de datos de rutas y hábitos del propio usuario y puede estar usando un software de IA generativa que provenga de un modelo fundacional (recogido en la *AI Act*). La futura legislación destinada solo a regular la circulación de los vehículos-robot y habilitar carriles especiales u ordenar las infraestructuras de 6G o la señalización quedaría incompleta si no contempla al AV como un extractor de datos del usuario. Y ese flanco está cubierto por la *AI Act* porque, aunque no hace referencia explícita a los vehículos autónomos, blinda el derecho de los usuarios a no convertirse en entrenadores no informados de la IA cuando aportan los datos de sus rutas a las plataformas dueñas de los vehículos para mejorar y optimizar sus programas. Por tanto, la combinación de las regulaciones de tráfico para los vehículos autopilotados y la aplicación de los derechos contemplados en la AI Act reducirán la asimetría entre los consumidores y las grandes plataformas que, previsiblemente, dominarán el mercado de los AVs. Sin embargo, por razones técnicas del aprendizaje profundo y por la propia opacidad de las empresas, será altamente improbable lograr, en la práctica, la trazabilidad exigida por la *AI*

Act a los productos de alto riesgo como el coche autónomo aunque, formalmente, las empresas presenten los resultados de sus ensayos y test obligatorios del AV como producto de alto riesgo.

V. BIBLIOGRAFÍA

AGRAWAL, Ajay, GANS, Joshua Y GOLDFARS, Avi, *Máquinas predictivas. La sencilla economía de la inteligencia artificial*, Barcelona, 2019. REM Reverté Management.

ATIENZA NAVARRO, María Luisa, *Daños causados por inteligencia artificial y responsabilidad civil*, Barcelona, 2022, Atelier Libros Jurídicos.

BANZI, Geofrey N., *Regulating Driverless Cars: A Concise Guide to the Driverless Future and Emerging Policy Issues in the UK*, GlobetEdit, 2017.

BONNEFON, Jean-François, SHARIFF, Azim y RAHWAN, Iyad, «The social dilemma of autonomous vehicles», *Science*, 2016, 352 (6293)

CGAE, *Inteligencia Artificial y Abogacía. Abogacía futura 2021: Prospectiva de Negocio Emergente*, 2020.

CHANNON, Matthew, McCORMICK, Lucy y NOUSSIA, Kyriaki, *The Law and Autonomous Vehicles (Contemporary Commercial Law)*, Nueva York, 2019, Informa Law from Routledge.

COCA-VILA, Ivón, «Self-driving Cars in Dilemmatic Situations: An Approach Based on the Theory of Justification in Criminal Law». *Cuadernos de Política Criminal*, Vol. 12 (2), 2018

COMISIÓN EUROPEA, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts*, COM/2021/206 final.

COMISIÓN EUROPEA, *Libro blanco sobre la inteligencia artificial- un enfoque europeo orientado a la excelencia y la confianza*, Bruselas, 2020.

COTINO HUESO, Lorenzo y TODOLÍ SIGNES, Adrián (coordinadores*), Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente*, Valencia, 2020, Tirant lo Blanch.

DIXON, Liza «Autonowashing: The Greenwashing of Vehicle Automation», publicado en *Transportation Research Interdisciplinary Perspectives*, Elsevier Ltd. 2020.

GARCÍA SEGURA, Luis A. y CAYÓN PEÑA, Juan, «Retos jurídicos de los vehículos conectados en la era del internet de las cosas», *Bol. Mex. Der. Comp.* vol.52 no.154 México ene./abr. 2019.

Gobierno del Reino Unido, *Rules on Sale Use of Automated Vehicles on GB roads*, Department for Transport, 25 de abril del 2022.

HERDMAN, Patricia, *When Cars Decide to Kill: Time por Software Safety Laws*, Toronto. Ethi-teque Inc, 2016.

HUERGO LORA, Alejandro José y DÍAZ GONZÁLEZ, Gustavo Manuel, *La regulación de los algoritmos*, Navarra, 2020, Thomson Reuters Aranzadi.

LEE, Kai-Fu, *Superpotencias de la inteligencia artificial*, Barcelona, 2020, Ed. Deusto.

LESSIG, Lawrence, *Code is law*, Harvard Magazine.

LOZANO AMÓSTEGUI, Cristina, *Un estudio sobre la conducción autónoma y su problemática jurídica*, Salamanca, 2020, Facultad de Derecho, Universidad Pontificia de Comillas.

MENECEUR, Yannick, *L'intelligence artificielle en procès*, Bruselas. Éditions Bruylant.

NOGUÉRO, David, «Intelligence Artificiale et vehicules autonomes». En BENSAMOUN, A. y Loiseau, G. *Droit de l'intelligence artificialle*. Cuaderno Les intégrales, número 15, Issy-les-Moulineaux Cedex, Editorial LGDJ Lextenso, 2019.

PASQUALE, Frank, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge (MA) y Londres, 2015, Harvard University Press.

PASQUALE, Frank, *New Laws of Robotics. Defending Human Expertise in the Age of IA*, Cambridge (MA), 2020. Harvard University Press.

SMITH, Bryant Walker, *Automated vehicles are probably legal in the United States*, The Center for Internet and Society, 2012.

TAEIHAGH, Araz y LIM, Hazel Si Min, *Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks*. Singapur. Transports Review, 2018.

UNITED STATES CONGRESS, «Self-Driving Cars: Levels of Automation Hearing before the Subcommitte on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce», *CreateSpace Independent Publishing Platform*, 2017.

UNIÓN EUROPEA, «Road safety in the EU: fatalities in 2021 remain well below pre-pandemic level», 28 de marzo de 2022.

WILLIAMS, James, *Clics contra la humanidad. Libertad y resistencia en la era de la distracción tecnológica*, Barcelona, 2021, Gatopardo.

WYLIE, Christopher, *Mindf*ck. Cambridge Analytica. La trampa para desestabilizar el mundo*, Barcelona, 2020, RocaEditorial de Libros.

WOLMAR, Christian, *Driverless Cars. One Road to Nowhere?,* Londres, 2020, London Publishing Partnership.

YIFANG, Ma, ZHENYU, Wang, HONG, Yang y LIN, Yang, «Artificial Intelligence Applications in the Development of Autonomous Vehicles: A Survey», *IEEE/CAA J. Autom. Sinica*, marzo de 2020, vol. 7, no. 2.

ZUBOFF, Shoshana, *La era del capitalismo de vigilancia*, Barcelona, Paidós, 2020.

LEGISLACIÓN APLICABLE EN LAS INTERACCIONES DE ACTORES EN UN COCHE AUTÓNOMO