COLECCIÓN
DERECHO
DEONTOLOGÍA
TECNOLOGÍA

La Colección Derecho. Deontología. Tecnología está destinada al análisis científico, dogmático, técnico y práctico de las más variadas ramas del ordenamiento jurídico en clave deontológica y tecnológica.

La temática de la Colección es heterogénea con un claro predominio del abordaje de la Justicia -Derecho procesal- desde una perspectiva poliédrica gracias a la diversidad de ramas del ordenamiento jurídico -Derecho civil, penal, administrativo, laboral, militar- comprometidas en su marco de acción. En esta Colección, se trabaja el Derecho desde una concepción esencialmente dogmática, pero también práctica. A su vez, una buena parte los libros -tanto de autoría única como colectivos- que integran esta colección no se realizan desde una exclusiva óptica jurídica, sino que afrontan incursiones en la (imprescindible) deontología jurídica de los distintos profesionales que nos dedicamos al Derecho (en general) y a la Justicia (en particular). Y todo ello en clave tecnológica, puesto que el día a día de nuestros Juzgados y/o Tribunales, al igual que el de nuestras Notarías y Registros se encuentra en un tránsito hacia la completa digitalización de todas las actuaciones cotidianas que favorecen nuestra Justicia, tanto preventiva como reactiva.

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS:

DESAFÍOS EN LA ERA DIGITAL

El Reglamento (UE) 2024/1689 establece normas armonizadas para el diseño, desarrollo y uso de sistemas de IA en la UE, garantizando la protección de derechos fundamentales como la privacidad. Al tiempo, todos los operadores jurídicos subrayan la importancia de prácticas adecuadas para la gestión y protección de los datos. Los desafíos legales derivados de este contexto son abordados en esta obra interdisciplinar que recoge los resultados de las **IV Jornadas Internacionales: Inteligencia Artificial (IA) y Protección de Datos**, organizadas por Red Iberoamericana de Investigación Interuniversitaria para el Diálogo Jurídico entre Europa y América (REDIJEA) y celebradas en la UNED.

DIRECTORES

Nayiber Febles Pozo y Patricia Nieto Rojas

AUTORES

Encarnación Abad Arenas, Carmen Maravilla Ares Vidal, Moisés Barrio Andrés, Pablo Fernández Alonso, Ana García García, Luis Miguel González De La Garza, Nayiber Febles Pozo, Ana I. González Fernández, Inmaculada Jiménez-Castellanos Ballesteros, Antonio Merchán Murillo, Patricia Nieto Rojas, M.ª Carmen Núñez Zorrilla, Tamara Prieto Pérez, Francisco Manuel Silva Ardanuy, Alejandro Zornoza Somolinos y Paola Zouak Lara

Proyectos de Investigación: «**Ejes de la Justicia en tiempos de cambio**», IP Sonia Calaza (PID2020-113083GB-I00), Ayuda PID2020-113083GB-I00 ayuda financiado/a por MCIN/AEI/10.13039/501100011033; «**Transición Digital de la Justicia**», IP Sonia Calaza (RED 2021-130078B-100), Ayuda Referencia TED2021-130078B-I00 ayuda financiado/a por MCIN/AEI/10.13039/501100011033 y por la «Unión Europea NextGenerationEU/PRTR»; y «**RED DE INVESTIGACIÓN: Alianzas estratégicas de la Justicia: Educación, Igualdad e Inclusividad**» (RED2024-153961-T), coordinada por Sonia Calaza, Programa Estatal de Transferència y Colaboración del Ministerio de Ciencia, Innovación y Universidades, Plan Estatal de Investigación Científica, Técnica y de Innovación 2024-2027.

PVP: 35,00 €
ISBN: 979-13-7011-111-3

COLECCIÓN DERECHO / DEONTOLOGÍA / TECNOLOGÍA

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS: DESAFÍOS EN LA ERA DIGITAL

3

COLEX

COLECCIÓN
DERECHO
DEONTOLOGÍA
TECNOLOGÍA

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS:

DESAFÍOS EN LA ERA DIGITAL

Directores

Nayiber Febles Pozo
Patricia Nieto Rojas

COLEX

Ayudando a los juristas desde 1981

RECURSOS A TU ALCANCE:

CÓDIGOS BÁSICOS

CÓDIGOS COMENTADOS

GUÍAS PASO A PASO

MONOGRAFÍAS

VADEMECUM

LIBROS DE BOLSILLO

BIBLIOTECA DIGITAL

FORMACIÓN

Descúbrelos en www.colex.es

Disfrute gratuitamente **DURANTE UN AÑO** de los eBook y audiolibros de las obras de Editorial Colex*

- Acceda a la página web de la editorial **www.colex.es**
- Identifíquese con su usuario y contraseña. En caso de no disponer de una cuenta regístrese.
- Acceda en el menú de usuario a la pestaña «Mis códigos» e introduzca el que aparece a continuación:

RASCAR PARA VISUALIZAR EL CÓDIGO

- Una vez se valide el código, aparecerá una ventana de confirmación y su eBook y/o audiolibro estará disponible **durante 1 año desde su activación** en la pestaña «Mis libros» en el menú de usuario.

* Los audiolibros están disponibles en las ediciones más recientes de nuestras obras. Se excluyen expresamente las colecciones «Códigos comentados», «Biblioteca digital» y los productos de www.vademecumlegal.es.

No se admitirá la devolución si el código promocional ha sido manipulado y/o utilizado.

¡Gracias por confiar en nosotros!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook

Acceso desde cualquier dispositivo con conexión a internet

Idéntica visualización a la edición de papel

Navegación intuitiva

Tamaño del texto adaptable

Síguenos en:

COLECCIÓN
DERECHO. DEONTOLOGÍA. TECNOLOGÍA

3

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS: DESAFÍOS EN LA ERA DIGITAL

Proyectos de Investigación: **«Ejes de la Justicia en tiempos de cambio»**, IP Sonia Calaza (PID2020-113083GB-I00), Ayuda PID2020-113083GB-I00 ayuda financiado/a por MCIN/ AEI/ 10.13039/501100011033; **«Transición Digital de la Justicia»**, IP Sonia Calaza (RED 2021-130078B-100), Ayuda Referencia TED2021-130078B-I00 ayuda financiado/a por MCIN/ AEI/ 10.13039/501100011033 y por la «Unión Europea NextGenerationEU/PRTR»; y **«RED DE INVESTIGACIÓN: Alianzas estratégicas de la Justicia: Educación, Igualdad e Inclusividad»** (RED2024-153961-T), coordinada por Sonia Calaza, Programa Estatal de Transferencia y Colaboración del Ministerio de Ciencia, Innovación y Universidades, Plan Estatal de Investigación Científica, Técnica y de Innovación 2024-2027.

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
AGENCIA ESTATAL DE INVESTIGACIÓN
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
UNED

COLECCIÓN
DERECHO. DEONTOLOGÍA. TECNOLOGÍA

3

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS: DESAFÍOS EN LA ERA DIGITAL

Directores

Nayiber Febles Pozo
Patricia Nieto Rojas

COLEX 2025

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, C.P. 15004
info@colex.es
www.colex.es

I.S.B.N.: 979-13-7011-111-3
Depósito legal: C 929-2025
DOI: https://doi.org/10.69592/979-13-7011-111-3

SUMARIO

CAPÍTULO 3

EL DESAFÍO DEL DERECHO ANTE LOS RIESGOS INVISIBLES DE LA INTELIGENCIA ARTIFICIAL EN LA RESOLUCIÓN DE CONFLICTOS

Ana I. González Fernández

CAPÍTULO 4

INSTRUMENTOS DE DEMOCRACIA ELECTRÓNICA PARTICIPATIVA ESTRUCTURADA POR LA IA. POSIBILIDADES Y LIMITACIONES

Luis Miguel González de la Garza

CAPÍTULO 5

LA DIFÍCIL CONVIVENCIA ENTRE LA INTELIGENCIA ARTIFICIAL Y LOS DERECHOS FUNDAMENTALES: LA TECNOLOGÍA *DEEPFAKE*

Inmaculada Jiménez-Castellanos Ballesteros

CAPÍTULO 6

IMPACTO DE LA DISCRIMINACIÓN DIRECTA E INDIRECTA DERIVADA DEL SESGO ALGORÍTMICO EN EL ÁMBITO DE LOS DERECHOS FUNDAMENTALES: ALCANCE Y PROTECCIÓN CONSTITUCIONAL

Francisco Manuel Silva Ardanuy

CAPÍTULO 7

VEHÍCULOS AUTOMATIZADOS E INTELIGENCIA ARTIFICIAL EN EL DERECHO DE DAÑOS: ENTRE EL SEGURO OBLIGATORIO Y EL PRODUCTO DEFECTUOSO

Alejandro Zornoza Somolinos

CAPÍTULO 8

LA IMPORTANCIA DE LA CIBERSEGURIDAD EN LOS VEHÍCULOS AUTÓNOMOS Y SU PROTECCIÓN EN LA LEGISLACIÓN EUROPEA

M.ª Carmen Núñez Zorrilla

CAPÍTULO 9

LA CONFLICTIVA CONVIVENCIA ENTRE INTERESES EMPRESARIALES Y DERECHOS COLECTIVOS EN LA EMPRESA INTELIGENTE

Ana García García

CAPÍTULO 10

DESAFÍOS ÉTICOS Y LEGALES DE LA INTELIGENCIA ARTIFICIAL EN EL MUNDO LABORAL

Tamara Prieto Pérez

CAPÍTULO 11

PLATAFORMAS DIGITALES Y SINDICATOS. ALGUNAS IDEAS PARA EL DEBATE TRAS LA APROBACIÓN DE LA DIRECTIVA 2024/2381

Patricia Nieto Rojas

CAPÍTULO 12

PLATAFORMAS DE RESOLUCIÓN DE CONFLICTOS ASISTIDAS POR IA: OPORTUNIDADES Y DESAFÍOS EN EL MARCO DE LA LEY ORGÁNICA 1/2025

Carmen Maravilla Ares Vidal

CAPÍTULO 13

LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA: CUESTIONES DE DERECHO INTERNACIONAL PRIVADO

Nayiber Febles Pozo

CAPÍTULO 14
PROPIEDAD, DATOS Y PODER EN LA ERA DE LA IA

Antonio Merchán Murillo

CAPÍTULO 15
LA PROTECCIÓN DE DATOS EN LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL: IMPLICACIONES EN EL DERECHO PENAL ESPAÑOL

Pablo Fernández Alonso

CAPÍTULO 16
SINERGIAS ENTRE EL RGPD Y LA IA EN EL ÁMBITO SANITARIO PARA LA TOMA DE DECISIONES AUTOMATIZADAS

Paola Zouak Lara

CAPÍTULO 8

LA IMPORTANCIA DE LA CIBERSEGURIDAD EN LOS VEHÍCULOS AUTÓNOMOS Y SU PROTECCIÓN EN LA LEGISLACIÓN EUROPEA[1]

M.ª Carmen Núñez Zorrilla

Profesora Titular de Derecho Civil.
Universidad Autónoma de Barcelona

1. Los nuevos riesgos de ciberseguridad en los vehículos autónomos. El reto de encontrar un equilibrio normativo entre la privacidad y la innovación hacia la transición digital

Se camina a nivel global hacia la automatización total de los vehículos o vehículos sin conductor, escalando hacia niveles de autonomía[2] cada vez

1 Este trabajo se ha realizado en el marco del Proyecto de Generación de Conocimiento 2021. Modalidad: Investigación No orientada Tipo B. PID2021-123070NB-I00, (I+ D), (2022-25), financiado por el Ministerio de Ciencia e Innovación, que lleva por título: *Conducción autónoma y seguridad jurídica del transporte*. IP. Eliseo Sierra Noguero.

2 Fundación Capgemini, *Libro Blanco para un vehículo autónomo inclusivo,* 2025, pp. 8 a 12, Disponible en https://www.capgemini.com/es-es/?s=Libro%20Blanco&paged=1&SortByDate=0

mayores. Actualmente, el sector del automóvil está experimentando una transformación estructural a una velocidad y de una magnitud sin precedentes. La experiencia del conductor y del pasajero en el vehículo está cada vez más definida por el *software* con inteligencia artificial (IA) y por la conectividad, con nuevas aplicaciones, como la conducción automatizada y autónoma, que desempeñan un papel cada vez más importante hacia la movilidad limpia, transformando el sector de la automoción[3].

El transporte avanzado y conectado es un concepto que engloba el uso de las altas tecnologías **para mejorar la eficiencia, la seguridad, la sostenibilidad y la accesibilidad de los sistemas de movilidad.** Entre los beneficios que aporta a la movilidad en general pueden destacarse: - la reducción del consumo de energía y las emisiones de gases de efecto invernadero, al optimizar las rutas, el tráfico y el uso compartido de vehículos; - la mejora de la seguridad vial, al prevenir y mitigar los accidentes mediante la detección y alerta de riesgos, la asistencia a la conducción y la automatización de funciones; - el aumento de la comodidad y el bienestar de los usuarios, al ofrecer servicios personalizados, información en tiempo real, entretenimiento y opciones de movilidad multimodal; - favorece la inclusión social, al facilitar el acceso a la movilidad a personas con discapacidad, de avanzada edad o con movilidad reducida o sin vehículo propio, e - impulsa la competitividad y la innovación, al generar nuevas oportunidades de negocio, empleo y desarrollo tecnológico[4].

No es necesario alcanzar la plena autonomía en la conducción para constatar que los coches hoy ya son centros de datos rodantes, hiperconectados y gobernados por *software*, donde cada decisión, desde la ruta óptima hasta el consumo energético, es gestionada en tiempo real a través de miles de líneas de código, pero como sucede con todo avance tecnológico, la progresiva incorporación de la inteligencia artificial en los vehículos para aumentar su eficiencia, seguridad y comodidad está dando lugar paralelamente a nuevos riesgos y vulnerabilidades, entre los que destacan los relacionados con la protección de los datos y la privacidad de los usuarios y de terceros. El funcionamiento adecuado de la inteligencia artificial precisa del tratamiento de grandes cantidades de datos a través de su conexión a la red, aumentando su rendimiento y eficiencia a medida que se incrementa la información recopilada. Sin embargo, esta digitalización también introduce nuevos peligros, ya que cada componente digital es un posible punto de acceso para los ciber

3 Comisión Europea, Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Plan de Acción Industrial para el Sector Europeo del Automóvil (COM/2025/95 final), Bruselas, 5 de marzo de 2025. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52025DC0095

4 Porras, O, «Ciberseguridad para vehículos: transporte, conectividad, conceptos y especificaciones tecnológicas», 2025, Disponible en https://www.securityinthenet.com/ciberseguridad-para-vehiculos-transporte-conectividad-conceptos-y-especificaciones-tecnologicas/

atacantes. Cuantos más dispositivos y sistemas interconectados, mayor es la superficie de ataque[5].

Los vehículos conectados están generando una cantidad creciente de datos, muchos de los cuales pueden ser considerados datos personales, ya que pueden ser relacionados con los conductores, los pasajeros, o incluso con terceros de forma directa o indirecta. Incluso cuando los datos no están relacionados directamente a un nombre sino a aspectos técnicos o funcionalidades del vehículo, podrían relacionarse con los usuarios del vehículo.

Un tipo de daño que está emergiendo con la utilización de esta tecnología es el que deriva de los ciberataques al vehículo. Ello es debido a que los vehículos autónomos conectados son plataformas tecnológicas complejas que dependen de sensores, sistemas de comunicación inalámbricos, redes y datos. La incorporación de tecnologías avanzadas hace que sea necesaria su conexión con grandes cantidades de datos, convirtiéndose en objetivos atractivos para los ciberdelincuentes[6] en un doble sentido: por un lado, son vulnerables al secuestro remoto, donde un pirata informático puede tomar el control total del automóvil[7], y por otro, son vulnerables a sufrir mayores intromisiones en la privacidad e intimidad de los usuarios del vehículo y de terceros, ya que al depender de su conexión a las redes para recopilar datos para su funcionamiento, abren una superficie más amplia para la posible entrada de los hackers.

El elemento esencial del vehículo conectado está en el tratamiento y uso de la información, que proviene tanto de los sensores del vehículo como de elementos externos, donde tanto el vehículo como el entorno intercambian información de manera inteligente, colectiva y cooperativa. A estas redes de transporte se las conoce como sistemas de transporte inteligentes y cooperativos. La evolución de estos sistemas en comunión con el vehículo automatizado dará lugar a la Conducción Conectada, Cooperativa y Automatizada[8].

Los vehículos autónomos dependen de la comunicación vehículo a todo (V2X) para interactuar con otros coches, infraestructuras y peatones. Dependiendo del tipo de enlace, existen principalmente los siguientes tipos de

5 S2GRUPO, *Segundo informe de ciberseguridad en vehículos eléctricos conectados 2025,* pp. 2, 5 y 39. Disponible en https://s2grupo.es/ciberseguridad-en-vehiculos-electricos-conectados/

6 ENISA (Agencia de la Unión Europea para la Ciberseguridad), *Guía de prácticas para para la seguridad de los coches inteligentes*, 2019, p. 16, Disponible en https://derechodelared.com/2019/12/24/enisa-publica-una-guia-de-buenas-practicas-y-recomendaciones-sobre-los-coches-conectados/

7 «La ciberseguridad en vehículos autónomos: retos y soluciones para un futuro seguro», Nota de prensa 2024, Disponible en https://www.hackrisk.cl/la-ciberseguridad-en-vehiculos-autonomos-retos-y-soluciones-para-un-futuro-seguro/

8 ANFAC, *Informe Vehículo Autónomo y Conectado,* 2023, p. 28, Disponible en https://anfac.com/publicaciones/informe-anfac-vehiculo-autonomo-y-conectado/

comunicaciones vehiculares con el entorno: - de vehículo a vehículo (V2V)[9] (Permite la comunicación del vehículo con los vehículos del entorno. El intercambio de datos entre éstos aumenta la seguridad en la carretera, evitando colisiones y reaccionando más rápido que el conductor, mejorando el consumo y el impacto medioambiental); - de vehículo a infraestructura (V2I)[10] (La comunicación entre el vehículo y la infraestructura vial urbana e interurbana, permite conectar los vehículos con infraestructuras viales - semáforos, farolas, cámaras, señales, carriles, parkings, peajes…- para optimizar el tráfico. A su vez, esta infraestructura puede conectarse e intercambiar información con los sistemas centrales de gestión del tráfico); - de vehículo a peatón (V2P)[11] (Esta comunicación permite a los usuarios vulnerables de la vía - peatones, ciclistas, personas en sillas de ruedas….- establecer comunicación con los vehículos a través de un terminal que permite detectar su presencia y alertar a los conductores para la prevención de accidentes); - de vehículo a red (V2N)[12] (La principal conexión de largo alcance del vehículo con el exterior se da entre el vehículo e Internet para a su vez conectarse a otros vehículos, infraestructuras y a los sistemas centrales de gestión del tráfico), y - de vehículo a la nube (V2C) (Se realiza a través de una conexión de banda ancha, como el 5G para aplicaciones como la actualización del software del vehículo, labores de diagnóstico o comunicación con aplicaciones que requieren de un volcado importante de datos)[13]. Todos estos mecanismos de comunicación se conocen colectivamente como «vehículo a todo» (V2X).

Para permitir las comunicaciones V2X, los vehículos están equipados con diferentes sistemas de comunicación inalámbrica, como las comunicaciones de corto alcance (DSRC40), la comunicación por luz visible (VLC), la comunicación por sensor de imagen (ISC), Wi-Fi o tecnologías de comunicación móvil, como 3G, 4G y 5G[14]. Si un hacker pudiera acceder a alguna de estas

9 González Prieto, A, *Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X*. Dir. por Jordi Serra Ruiz, Máster Universitario en Ciberseguridad y Privacidad, Universitat Oberta de Catalunya, 2022, p. 19.

10 Intercambio de información entre el vehículo y la infraestructura de la vía. Los vehículos pueden recibir información de sensores instalados en la vía sobre el estado de los semáforos, accidentes, aparcamientos, etc. A su vez, el vehículo también envía información propia o reenvía la recibida de otros vehículos a la infraestructura, con el objetivo de mejorar la circulación y disminuir el número de accidentes; González Prieto, A, *Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X*, *op. cit.,* p. 20.

11 Los peatones también estarán preparados para comunicarse con el ecosistema, por ejemplo, por medio de aplicaciones móviles, de la presencia de bicicletas, sillas de ruedas o niños en las proximidades; González Prieto, A, *Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X, op. cit*., p. 20.

12 González Prieto, A, *Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X*, *op. cit.,* p. 20.

13 ANFAC, *Informe Vehículo Autónomo y Conectado, op. cit.,* p. 29.

14 ENISA (Agencia de la Unión Europea para la Ciberseguridad), *Guía de prácticas para para la seguridad de los coches inteligentes*, 2019, *op. cit*., pp. 13 a 15.

conexiones, podría manipular muchas funciones del coche. Podría, por ejemplo, activar o desactivar los frenos, manejar los volantes, aumentar la velocidad del vehículo, provocar fallos en el software[15], apagar el motor a distancia cuando el vehículo está en movimiento[16], acceder y arrancar un vehículo sin necesidad de la llave a través del **sistema de acceso sin llave (keyless), atacar el sistema de llamada de emergencia** para evitar que los servicios de emergencia asistan al usuario en caso de siniestro, o un ataque al **sistema eléctrico** o al punto de recarga, que podría provocar desde una costosa avería hasta un incendio[17]. El riesgo de piratería informática en la infraestructura de carga es otra preocupación apremiante, sobre todo porque intercepta con sistemas e infraestructuras informáticas críticas como la red eléctrica o las redes de backend[18]. Los hackers pueden causar interrupciones en el servicio, inutilizando los puntos de carga[19].

En general, entre los componentes críticos susceptibles de ser comprometidos se encuentran: - los Sistemas de Comunicación Vehicular: los vehículos autónomos se comunican con otros vehículos, infraestructuras y dispositivos. La interceptación o alteración malintencionada de estos datos puede llevar a desinformar al vehículo o, peor aún, a otorgar el control a un actor no autorizado; - Software y Firmware: la presencia de defectos de software, ya sean inherentes o inducidos por medio de actualizaciones maliciosas, puede resultar en un comportamiento impredecible del vehículo; - Sensores y Cámaras: los atacantes podrían manipular sensores o inyectar datos falsos, lo que resultaría en decisiones inadecuadas de navegación o detección de

15 CIBERSEGURIDAD, «Ciberseguridad en vehículos conectados y autónomos», Nota de prensa, 2024, Disponible en https://ciberseguridad.com/guias/industrial/vehiculos-conectados-autonomos/

16 UNE (Normalización Española), «Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno Disponible en https://revista.une.org/37/normalizacion-en-ciberseguridad-para-la-movilidad-inteligent.html », 2021, p. 5,

17 JOSESILVA. Correduría de Seguros, «La ciberseguridad de los vehículos conectados», 2023, Disponible en https://josesilva.es/ciberseguridad-vehiculos-conectados/

18 UPSTREAM, *Informe de ciberseguridad global sobre movilidad inteligente y automotriz 2025*, Disponible en https://upstream.auto/ty-upstreams-2025-global-automotive-cybersecurity-report/?utm_campaign=6809247-2025%20Global%20Automotive%20Cyber%20Trends%20Report&utm_medium=email&_hsenc=p2ANqtz--eYGYNLzpMUiWe0HFi7uzIq-qKIvyh0KYjkvnZDrbeiOFuEJYcIKOYTIfP9suDwcJ1IWcGQjKmwF7JxDgrV11FxOQTOTA&_hsmi=346724713&utm_content=346724713&utm_source=hs_automation&hsCtaTracking=c28a2130-2e86-4a3f-ac19-1dc673f1ef98%7Cf8e9b23b-1a3a-443d-8d5d-e272ce62b311

19 Uno de los casos más graves se produjo en Lituania, donde un grupo de ciberdelincuentes tomó el control de una red de estaciones de carga de vehículos eléctricos, dejando sin servicio a miles de usuarios y filtrando datos de más de 20.000 clientes; Fernández, A, «Crecen los ciberataques a coches eléctricos y conectados», Coche global, Noticia de prensa, 2 de marzo de 2025, Disponible en https://www.cocheglobal.com/tendencias/crecen-ciberataques-coches-electricos-conectados_810141_102.html

obstáculos; - Sistemas de Propulsión y de Control: se pueden comprometer estos sistemas interfiriendo en operaciones críticas del vehículo como la dirección, el frenado y la aceleración[20].

A ello se le suma otra vulnerabilidad; los usuarios se enfrentan a amenazas a la privacidad, y es que los coches autónomos recopilan una gran cantidad de información personal de los pasajeros que puede ser utilizada por los hackers para actividades fraudulentas o para violar la privacidad de los usuarios, como la ubicación, los hábitos de conducción, las preferencias de entretenimiento[21], datos sobre qué es lo que está haciendo el usuario, un registro completo de los lugares que el usuario ha visitado o el seguimiento de todos sus movimientos. El hacker puede aprovecharse del sistema bluetooth para obtener un volcado de datos que le permitan conocer la posición de la víctima y espiarla, acosarla o suplantar su identidad[22]. En general, será posible rastrear todos los movimientos de los usuarios, así como los detallados datos de sus comportamientos y las preferencias personales. Permitirán también la creación de un retrato íntimo y muy complejo de un individuo, que incluye datos muy sensibles sobre hábitos, creencias, viajes, orientación sexual e ideología. Sin mencionar datos que podrían derivarse de la sincronización del dispositivo móvil con el automóvil, o de un vehículo con un dispositivo ubicado en la casa del usuario[23]. Los datos privados de los teléfonos inteligentes, como el correo electrónico, los mensajes de texto, los contactos y otros datos personales, podrían ser robados por los piratas informáticos a través del vehículo. La información sobre la ubicación de los vehículos incluso puede utilizarse para determinar cuándo están ausentes los ocupantes de una casa, dando a los ladrones una oportunidad[24].

---

20 ITC Web Solutions, «La ciberseguridad en vehículos autónomos: riesgos y soluciones», Nota de prensa, 2024, Disponible en https://itcwebsolutions.com/tecnologia-y-tendencias/drones-y-vehiculos-autonomos/regulacion-y-seguridad/la-ciberseguridad-en-vehiculos-autonomos-riesgos-y-soluciones/#:~:text=La%20ciberseguridad%20en%20veh%C3%ADculos%20aut%C3%B3nomos%3A%20riesgos%20y%20soluciones,...%203%20Proyecciones%20Futuras%20y%20Desarrollo%20Continuo%20

21 Historia de la Tecnología, «La ciberseguridad en los vehículos autónomos: desafíos y soluciones», Nota de prensa 2024, Disponible en https://techevolucion.net/transporte-y-movilidad/ciberseguridad-vehiculos-autonomos-desafios-soluciones/

22 JOSESILVA, Correduría de Seguros, «La ciberseguridad de los vehículos conectados», *op. cit.*

23 Lubomira Kubica, M, «Vehículos autónomos y la privacidad: una perspectiva norteamericana», en Sancho López y Martínez Velencoso, *Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación*, Aranzadi, 2022, Disponible en https://legalteca-aranzadilaley-es.eu1.proxy.openathens.net/LinkToPublication?publication=10021109_00000000_0&fileName=e_Capitulo07.xhtml&location=pi-3886&searchHighlight=ciberseguridad%20veh%C3%ADculos%20aut%C3%B3nomos

24 UNE (Normalización Española), «Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno», *op. cit*., p. 5.

En definitiva, son principalmente dos los riesgos asociados con la piratería de vehículos autónomos: 1) el hacker puede tomar el control del automóvil de forma remota[25], y 2) el hacker puede acceder a la información personal de los usuarios[26].

Las ciber amenazas en el contexto de los vehículos autónomos conectados evolucionan a un ritmo mayor al que la industria está preparada para gestionar, superando las medidas regulatorias. Las regulaciones actualmente existentes sobre ciberseguridad en los vehículos autónomos todavía son insuficientes para abordar las amenazas dinámicas y complejas a las que se enfrenta este ecosistema. Se observa un aumento constante de los riesgos cibernéticos con graves consecuencias para la seguridad, la reputación de la marca, la continuidad operativa, la privacidad de los datos y la estabilidad financiera. El auge de los vehículos autónomos definidos por *software* está introduciendo nuevas vulnerabilidades, ampliando la superficie de ataque[27].

Al mismo tiempo sucede que la gestión de la movilidad inteligente cambia la perspectiva tradicional de la protección de la privacidad por una nueva marcada por la tecnología y las nuevas formas de operar digitalmente. La inteligencia artificial, el Internet de las Cosas[28], el Big data, y, en general, cualquier tecnología avanzada como la que se incorpora en los vehículos totalmente automatizados, necesita recopilar datos masivos para funcionar de manera eficaz, a menudo personales, y este hecho es difícil de compaginar con la aplicación estricta de los criterios y principios que sustentan la normativa tradicional sobre protección de datos, que fue elaborada sin tenerse en cuenta las características que definen a los productos en la era digital.

---

25 Poniendo en peligro la vida de los ocupantes del vehículo o de terceros.

26 Provocando una vulneración de la intimidad del propietario o usuario del vehículo.
CIBERSEGURIDAD, «Ciberseguridad en vehículos conectados y autónomos», Nota de prensa, 2024, Disponible en https://ciberseguridad.com/guias/industrial/vehiculos-conectados-autonomos/

27 UPSTREAM, *Informe de ciberseguridad global sobre movilidad inteligente y automotriz 2025, op. cit.,* p. 1.
CIBER PROTEGIDOS, «El impacto de los coches autónomos en las estrategias de ciberseguridad», Disponible en https://cyberprotegidos.info/retos-futuros/impacto-coches-autonomos-estrategias-ciberseguridad/

28 El **Internet de las cosas** (IoT) es un sistema tecnológico que permite que **los objetos se conecten a Internet y entre sí.** Incluye cualquier objeto o «cosa» que pueda conectarse de manera inalámbrica a una red de Internet. Pero hoy en día, IoT se refiere más específicamente a cosas conectadas que están equipadas con sensores, software y otras tecnologías que les permiten transmitir y recibir datos —con el propósito de informar a los usuarios o automatizar una acción—. Tradicionalmente, la conectividad se lograba principalmente a través de wi-fi, mientras que hoy el 5G y otros tipos de plataformas de red ofrecen la promesa de manejar enormes data sets, casi en cualquier lugar, con velocidad y confiabilidad; SAP, «¿Qué es internet de las cosas (IoT)?», Disponible en https://www.sap.com/spain/products/technology-platform/what-is-iot.html

Desde la Comisión Europea se considera que los datos de movilidad son un potente motor para mejorar la innovación y la eficiencia, reducir el impacto medioambiental y mejorar la calidad de vida de todos los europeos. Aprovechar estos datos puede conducir a una planificación más inteligente y resiliente de las infraestructuras y los servicios de transporte, a un tráfico más fluido, a viajes transfronterizos más fáciles, a cadenas logísticas más competitivas y a una presentación de informes más sencilla por parte de las pymes. Más allá de la simple recopilación de datos, el desafío estriba, asimismo, en hacer que sea más fácil compartirlos de una manera segura y controlada, y transformarlos en inteligencia procesable. Se trata de aprovechar el potencial de los datos del transporte para apoyar el desarrollo de la IA y otras tecnologías de vanguardia[29]. Por ello, es necesario actualizar la normativa en materia de protección de datos, que no se creó pensando específicamente en la inteligencia artificial, para adaptarla a la nueva realidad y tomar en consideración aspectos que no se tuvieron en cuenta cuando la misma se elaboró. Se necesita un adecuado marco normativo actualizado que, teniendo en cuenta los nuevos riesgos que plantea esta tecnología emergente, sea capaz de encontrar un equilibrio entre la protección de la privacidad que requiere ser reforzada ante la ampliación de la superficie de ataque, y la innovación hacia una movilidad inteligente[30], que debe seguir avanzando por los muchos beneficios que también reportará. Un marco claro para el acceso a los datos de los vehículos liberaría todo el valor de este recurso, permitiendo a las empresas de toda la cadena de suministro contribuir a la excelencia de la automoción europea.

2. La respuesta normativa de la Unión Europea para brindar una protección adaptada a los nuevos riesgos de ciberseguridad en los vehículos altamente automatizados y su ejecución en la industria automovilística española

Desde la Unión Europea (UE) se reconocen los beneficios potenciales de los vehículos autónomos, haciendo que el transporte por carretera sea más

29 Comisión Europea, «Liberar el potencial de los datos de movilidad», Nota de prensa, 19-septiembre-2024, Disponible en https://digital-strategy.ec.europa.eu/es/policies/mobility-data

30 Véase en tal sentido a España Pérez, J.A, «La problemática jurídica de la protección de datos en la Smart mobility. Especial referencia al Reglamento 2016/679», *Revista española de Derecho Administrativo 207*, julio-septiembre, 2020, Disponible en https://legalteca-aranzadilaley-es.eu1.proxy.openathens.net/LinkToPublication?publication=LEGAR05_00000000_20200701000002070000&fileName=243848015.html&location=pi-10428&searchHighlight=ciberseguridad%20en%20veh%C3%ADculos%20aut%C3%B3nomos

seguro, eficiente y respetuoso con el medio ambiente. Se reconoce que la conducción automatizada reducirá en gran medida el riesgo de error humano, ayudando de esta manera a que disminuya el número de víctimas mortales en la carretera, permitiendo optimizar la movilidad, reducir la congestión del tráfico y los costes del transporte, reducir drásticamente las emisiones de $CO2$[31], al mismo tiempo que permitirá a los pasajeros (ya no, conductores) poder dedicar el tiempo del transporte a otras ocupaciones[32]. Por ello, desde la UE se impulsa su desarrollo y despliegue; se quiere acelerar la transición hacia la conducción totalmente automatizada o autónoma para que la industria automovilística europea sea competitiva a escala mundial. Con todo, se reconocen los nuevos riesgos de seguridad que ya están afectando y que afectarán directamente a las personas, por la creciente vulnerabilidad que representa esta nueva tecnología a los ciberataques.

El sistema de IA de la máquina se fundamenta, en gran medida, en la recopilación y procesamiento masivo de datos, lo cual es esencial para el entrenamiento de los algoritmos y la optimización de su precisión. **El tratamiento a gran escala de datos personales es una característica inherente de estos sistemas;** especialmente en aquellos basados en técnicas de Machine Learning y Deep Learning. La normativa europea en materia de protección de datos, como el *Reglamento General de Protección de Datos*[33] *(RGPD)*, exige que dicho tratamiento se sustente en una base jurídica adecuada, lo que en el ámbito de la IA suele requerir la obtención de un consentimiento explícito e informado de los titulares de los datos. Esta exigencia, en combinación con la naturaleza opaca de los sistemas de IA, plantea desafíos complejos en el contexto de los vehículos inteligentes en términos de conformidad legal.

El mayor riesgo al que quedan expuestas las personas que interactúan con estas tecnologías de sufrir violaciones a la intimidad y a la privacidad, debe compaginarse con un cambio de enfoque en las nuevas normas promovidas por la UE sobre datos, que, de poner el centro de la actividad legislativa exclusivamente en la protección de los derechos de los ciudadanos, se centran ahora asimismo en maximizar el valor de los datos digitales como activo esencial para la digitalización europea. Se trata también de fomentar su uso por el gran valor que pueden aportar a la economía y a la sociedad.

---

31 Dirección General de Tráfico, «Vehículos de conducción automatizada. Los vehículos de conducción automatizada representan una revolución para la movilidad del futuro», Nota de prensa. Disponible en https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/vehiculos-de-conduccion-automatizada/, 21 de marzo de 2024.

32 Lafuente Sánchez, R, *Inteligencia artificial y vehículos autónomos: responsabilidad civil extracontractual internacional*, *op. cit*., pp. 30 y 31.

33 Parlamento Europeo, *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),* en DOUE, 4-5-2016.

Este equilibrio entre la protección de los derechos en un contexto cada vez más vulnerable por la propia manera de funcionar de la nueva tecnología, y la necesidad y promoción cada vez más intensa de la compartición de los datos, supone un reto legislativo en el ámbito de la ciberseguridad de los coches autónomos para la UE de máxima prioridad.

La regulación europea de protección de datos personales (Reglamento General de Protección de Datos – RGPD) solo aborda el fenómeno de los datos de forma parcial y algunos de los principios en los que se fundamenta son de difícil aplicación en el ámbito de las tecnologías digitales con IA.

Así, la regulación tradicional se basa en el principio de minimización de datos, que implica que los responsables y encargados deben evitar el tratamiento de datos personales innecesarios o excesivos para la consecución de sus objetivos. Solo se deben recolectar los datos estrictamente necesarios para un propósito específico. En el caso de la IA, donde grandes volúmenes de datos son esenciales para entrenar algoritmos eficaces, este principio puede ser difícil de aplicar. La IA utiliza el aprendizaje automático (Maquine Learning) que permite que los sistemas aprendan de grandes cantidades de datos y mejoren con el tiempo. Además, los sistemas de IA pueden generar nuevos datos a partir de los datos de entrada, como perfiles, predicciones o recomendaciones, que pueden tener un impacto significativo en los derechos y libertades de los interesados[34].

El principio de proporcionalidad del RGPD exige que el tratamiento de datos sea adecuado, pertinente y limitado a lo necesario en relación con los fines para los cuales se procesan. En el contexto del Machine Learning y el Big Data[35], la recopilación de grandes volúmenes de datos a menudo excede lo necesario para el propósito específico declarado, ya que los algoritmos requieren de datos, no solo para cumplir con el propósito inmediato, sino también para mejorar su rendimiento con el tiempo. Sin embargo, el RGPD establece que los datos personales deben estar limitados solo a lo necesario,

34 Fernández, J. A, «El Reglamento (RGPD) y la inteligencia artificial», en *Seifti,* Nota de prensa de 12 de febrero de 2024, Disponible en https://seifti.io/es/el-reglamento-rgpd-y-la-inteligencia-artificial/

35 *Big Data* es el conjunto de tecnologías, prácticas y conceptos que permiten la recolección, almacenamiento, procesamiento y análisis de grandes volúmenes de datos que son demasiado complejos o extensos para ser gestionados con las herramientas tradicionales de gestión de datos. Estos datos pueden provenir de diversas fuentes, como redes sociales, sensores, transacciones comerciales, dispositivos IoT (Internet de las Cosas), entre otros. Se refiere a conjuntos de datos más grandes y complejos, especialmente provenientes de nuevas fuentes, que son tan voluminosos que las soluciones tradicionales de procesamiento de datos no pueden gestionarlos; Redondo Martín, J.A, «Qué es Big Data: Funcionamiento, Aplicaciones y Salidas Profesionales», *CEU,* 2025, Disponible en https://www.ceu.es/blog/2024/que-es-big-data-funcionamiento-aplicaciones-y-salidas-profesionales/

lo que puede entrar en conflicto con la práctica de recolectar grandes cantidades de datos que puedan ser útiles en el futuro[36].

Se pone en entredicho, asimismo, el principio del procesamiento justo, que requiere que el responsable del tratamiento deba tener en cuenta y justificar activamente por qué un algoritmo es justo y que el uso del algoritmo elegido no conduce a resultados inapropiados. Cuando un sistema de IA no es lo suficientemente transparente, es imposible que quienes supervisan su uso identifiquen sesgos en su razonamiento y salida.

El principio de finalidad que contempla el RGPD, según el cual, los datos personales deben recopilarse para fines específicos y explícitos, y no deben ser tratados posteriormente de manera incompatible con esos fines, también entra en conflicto con el enfoque del Big Data y el Machine Learning propios de la IA, donde los datos se recopilan masivamente y a menudo se reutilizan para fines no previstos inicialmente, como el desarrollo de nuevas funcionalidades o predicciones que no fueron explícitas en el momento de la recopilación[37].

Otro de los principios fundamentales del RGPD es el consentimiento informado. Las organizaciones deben informar sobre la finalidad del tratamiento y obtener el consentimiento explícito de los individuos antes de recolectar y procesar sus datos[38]. El principio de información obliga a los responsables del tratamiento a proporcionar a los interesados información clara, comprensible y accesible sobre cómo se procesan sus datos personales. En el caso de la inteligencia artificial y la toma de decisiones automatizadas, este principio es fundamental para garantizar la transparencia y permitir que los individuos comprendan cómo se procesan sus datos. El problema es que la naturaleza opaca de los algoritmos de IA hace difícil cumplir con el principio de información del RGPD. A medida que los modelos de IA se vuelven más avanzados, su capacidad para proporcionar explicaciones claras sobre cómo llegan a sus decisiones, disminuye, lo que contraviene el principio de que los interesados deben ser informados de manera inteligible sobre el tratamiento de sus datos. La opacidad inherente a los modelos de IA de «caja negra» hace que sea difícil para los responsables del tratamiento proporcionar información comprensible sobre cómo los algoritmos procesan los datos y llegan a deci-

---

36 GRUPO ATICO34, «Protección de Datos e Inteligencia Artificial», Disponible en https://protecciondatos-lopd.com/empresas/inteligencia-artificial/

37 **El Machine Learning** es una rama de la inteligencia artificial que permite que las máquinas aprendan de los datos sin ser programadas explícitamente para realizar tareas específicas. Los modelos de Machine Learning utilizan grandes conjuntos de datos para mejorar su precisión y tomar decisiones más eficientes con el tiempo; Véase GRUPO ATICO34, «Protección de Datos e Inteligencia Artificial», *op. cit*.

38 SOFTWARE, «Inteligencia artificial y protección de datos: cómo afecta el RGPD?», Noticia de prensa de 25-10-2024, Disponible en https://softwarelopd.com/blog/inteligencia-artificial-y-proteccion-de-datos-como-afecta-el-rgpd/

siones. Esto crea una barrera para que los usuarios comprendan el proceso y ejerzan sus derechos, como el derecho a la rectificación o el acceso a la información. Tampoco pueden impugnar efectivamente la decisión, ya que no tienen suficiente información sobre cómo se tomó. Esto afecta al derecho de los individuos a solicitar una explicación de la decisión automatizada, tal como lo establece el RGPD[39].

Por otra parte, el RGPD regula únicamente el tratamiento de los datos de naturaleza personal, esto es, los que se refieren a una persona física identificada o identificable, por lo que no alcanza a comprender los datos que no se refieran a personas físicas, dejando fuera de esta regulación a un gran número y categorías de datos digitales. Existe una gran cantidad de datos que también pueden recogerse en la máquina, que no tienen la consideración de datos personales (p. ej., datos puramente industriales, medioambientales, agrícolas o los financieros empresariales, entre muchos otros), que gozan también de un gran valor y tienen la capacidad de generar un gran crecimiento económico y social. Sin embargo, no han gozado del mismo nivel de regulación en Europa, por lo que su uso, protección y compartición han estado rodeados de gran incertidumbre e inseguridad jurídica. La regulación sobre protección de datos tradicional centra sus esfuerzos en otorgar una protección sólida a las personas físicas titulares de esos datos, pero obvia otras líneas de acción sobre los datos digitales, como las de promoción de un mercado europeo de datos o el fomento de la compartición y flujo de estos en aras a la digitalización. Es, por tanto, una regulación cuyos efectos en el tejido empresarial europeo implican más la existencia y exigencia de límites a la compartición de los datos que un incentivo a hacerlo.

Por todo ello, sin olvidar ni aparcar la protección que otorga el RGPD, que sigue vigente y que deberá continuar siendo aplicado en todo caso, la nueva normativa promovida por la UE plantea un nuevo enfoque, que es el de promover la posibilidad de que los datos, personales o no, puedan ser compartidos entre los actores económicos y sociales para hacer crecer la sociedad y economía digitales en Europa. Esta nueva línea de actuación debe además compaginarse con la mayor vulnerabilidad que presenta esta tecnología a sufrir ciberataques. Es por estos motivos que la regulación parcial e insuficiente de los datos que proporciona el RGPD está siendo completada y ampliada actualmente con nuevas normas europeas que buscan promover la digitalización en Europa y crear ese mercado europeo de datos, impulsando su compartición. Aborda y establece reglas aplicables a los datos como activo digital, sean de carácter personal o no[40].

39 GRUPO ATICO34, «Protección de Datos e Inteligencia Artificial», *op. cit*.

40 López-Lapuente, L, «La nueva regulación europea de los datos: cómo dar forma al futuro digital de Europa», *Actualidad Jurídica Uría Menéndez,* n.º 61, 2023, pp. 51 a 59.

Ante esta panorámica y siendo consciente de los peligros expuestos, desde la UE se han presentado iniciativas legislativas posteriores al RGPD[41], que lo complementan y que, reconocen la creciente importancia de la protección de la privacidad en la era digital. Entre estas iniciativas, por su incidencia en los vehículos autónomos, deben mencionarse las siguientes:

La *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)*, de 10-enero de 2017[42], también denominado Reglamento ePrivacy. Busca actualizar y reemplazar a la Directiva ePrivacy de 2002, adaptándose a los avances tecnológicos y a las nuevas formas de comunicación que han surgido en las últimas décadas. La **Directiva ePrivacy** se diseñó en un contexto en el que las telecomunicaciones estaban dominadas por proveedores de redes y servicios de telecomunicaciones convencionales. Sin embargo, el **Reglamento ePrivacy** responde a la evolución del ecosistema digital y abarca una categoría más amplia de actores, incluyendo proveedores de servicios de comunicaciones electrónicas basados en Internet.

El Reglamento ePrivacy es una ley especial dentro de una ley general que es el Reglamento General de Protección de Datos, que complementa a éste con normas que se aplican específicamente al sector de las comunicaciones electrónicas. Además, el Reglamento **ePrivacy prevalecerá sobre el RGPD** en las áreas específicas que cubre. El RGPD cubre el derecho a la protección de los datos personales, mientras que el Reglamento ePrivacy abarca el derecho de una persona a una vida privada, incluyendo la confidencialidad, en todo tipo de comunicaciones electrónicas. En el mismo se considera que el contenido de las comunicaciones electrónicas puede desvelar información muy delicada sobre las personas físicas que participan en ellas, tales como experiencias personales y emociones, problemas de salud, preferencias sexuales y opiniones políticas, cuya divulgación podría causar daños personales y sociales, pérdidas económicas o situaciones embarazosas. Entre estos metadatos figuran los números a los que se ha llamado, los sitios web visitados, la localización geográfica o la hora, la fecha y la duración de una llamada, información que permite extraer conclusiones precisas sobre la vida privada de las personas participantes en la comunicación electrónica tales como sus

41 Rubí Puig, A, «Inteligencia artificial y daños indemnizables», Capítulo XI, en Álvarez Lata, N, *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, 2024, p. 657.

42 Parlamento Europeo, *Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas),* 2017, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010&qid=1744477392736

relaciones sociales, sus costumbres y actividades de la vida cotidiana, sus intereses, sus preferencias, etc. Estos datos también pueden revelar información relativa a las personas jurídicas, como secretos comerciales u otro tipo de información confidencial que tiene valor económico.

Con el fin de garantizar la plena protección de los derechos a la privacidad y la confidencialidad de las comunicaciones y promover una Internet de las cosas fiable y segura en el mercado único digital, el Reglamento será también de aplicación a la transmisión de comunicaciones de máquina a máquina[43].

Refuerza el régimen sancionador en caso de incumplimiento, alineándose con las **sanciones establecidas en el Reglamento General de Protección de Datos**, y promueve una mayor transparencia en el ecosistema digital, obligando a las empresas a informar de manera clara y accesible sobre cómo recopilan, procesan y almacenan los datos de los usuarios. Esta mayor exigencia en la rendición de cuentas contribuirá a fortalecer la confianza de los consumidores en el entorno digital, fomentando una relación más equilibrada entre usuarios y proveedores de servicios digitales. Supone un avance clave en la regulación de la privacidad online, equilibrando la innovación tecnológica con la protección de los derechos fundamentales en el entorno digital[44]. Cabe decir que actualmente todavía es una Propuesta que se encuentra en fase de negociación entre el Consejo de la UE, el Parlamento Europeo y la Comisión Europea. Mientras siga siendo un borrador se aplica la Directiva ePrivacy, que aborda específicamente los problemas de privacidad en las comunicaciones electrónicas.

El Comité Europeo de Protección de Datos (CEPD) adoptó el 7 de octubre de 2024, la versión final de las *Directrices 2/2023 sobre el alcance técnico del art. 5.3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo —Directiva ePrivacy—, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*. En virtud de estas Directrices, el CEPD amplía la aplicación de la Directiva para el almacenamiento o el acceso a la información en el dispositivo de un usuario.

El objetivo de las Directrices es proporcionar una comprensión clara de las operaciones técnicas cubiertas por el artículo 5, apartado 3, de la Directiva e-Privacy, con el ánimo de resolver la ambigüedad sobre la aplicación de

---

43 B. Fernandez, C, «Contenido de la propuesta de Reglamento europeo sobre privacidad de las comunicaciones electrónicas», en *Diario La Ley*, Wolters Kluwer, 3-5-2017, Disponible en https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1czUwMDA0sjQ2sDBVK0stKs7Mz7M1MjA0NzA1MFbLy09JDXFxti3NS0lNy8xLTQEpyUyrdMlPDqksSLVNS8wpTlVLTcrPz0YxKR5mAgCGzyCmYwAAAA==WKE

44 Grupo Adaptalia, *Reglamento ePrivacy: qué es y cómo impacta en la privacidad online,* Nota de prensa, 14-3-2025, Disponible en https://grupoadaptalia.es/blog/reglamento-eprivacy-2/

la norma a nuevas tecnologías de seguimiento que han proliferado como alternativa a herramientas generalmente utilizadas. Las Directrices proporcionan los elementos clave para clarificar la interpretación del artículo 5.3 de la Directiva e-Privacy, reafirmando la importancia de proteger la privacidad de los usuarios en el entorno digital actual, donde las tecnologías de seguimiento son cada vez más sofisticadas[45].

El *Reglamento (UE) 2019/881 relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad)*[46], de 17 de abril de 2019, que establece un marco europeo de certificación de la ciberseguridad para mejorar el funcionamiento del mercado interior por medio del aumento de la ciberseguridad en la UE y permitir un enfoque armonizado de cara a los esquemas europeos de certificación de la seguridad, con vistas a la creación de un mercado único digital para productos, servicios y procesos de TIC, permitiendo que los certificados de ciberseguridad europeos y las declaraciones de conformidad de la UE de productos, servicios o procesos de TIC sean reconocidos y usados en todos los Estados miembros[47].

En enero de 2024, la Comisión Europea adoptó el Reglamento de Ejecución (UE) 2024/482[48], que entró en vigor el 27 de febrero de 2025. Este acto establece normas para la aplicación del Reglamento (UE) 2019/881 en lo que respeta a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes. Se trata del primer esquema a escala de la UE referente a certificados de los niveles de garantía «sustancial» o

45 ECIJA, *Directrices 2/2023 sobre el alcance técnico del art. 5.3 de la Directiva ePrivacy,* 19-12-2024, Sala de prensa, pp. 1,2,3 y 6, Disponible en https://ecija.com/sala-de-prensa/directrices-2-2023-sobre-el-alcance-tecnico-del-art-5-3-de-la-directiva-eprivacy/

46 *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («Reglamento sobre la Ciberseguridad»)*, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32019R0881

47 Diario La Ley Wolters Kluwer, «Publicado el Reglamento sobre ciberseguridad de la Unión Europea», 10-6-2019, Disponible en https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAC2NwW7CMBBEv6a-VEIOEgQOe0nhhhBqI-4be5VYSrzgXafk72sKh9FqtG9m7pnS0tJDwXGUPAXP6ZOmWyJBI-0vkuEzQpkxGsROwH7WritYGnWYcD-ygrvZPF2ZqsYO14eQpNQtYo6w4fpPAdrcxMvD-vGefQowaODaZXbfAezkdrbbXfVNt6Z2ZKUgC4hp6ikhlCP5yK9MULYXLDBXuCMp6nw-vAK5fZ4f5qsWtKdxp9_b9xY7gGVvnCk6N-7f0wP10X4AAAAWKE

48 *Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC),* Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32024R0482

«elevado» para productos de TIC como «hardware» y «software», incluidos los componentes como chips y tarjetas inteligentes.

Las *Directrices 1/2020, sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad*[49], en las que partiendo de la cada vez mayor conectividad de los vehículos, que genera cantidades de datos cada vez mayores, la mayoría de los cuales pueden considerarse datos personales relacionados con los conductores o pasajeros, tienen por objeto facilitar el cumplimiento del tratamiento de los datos personales realizado por una amplia gama de partes interesadas que operan en este entorno. El ámbito de aplicación de estas Directrices se centra en el tratamiento de los datos personales en relación con el uso no profesional de vehículos conectados por parte de los interesados: por ejemplo, conductores, pasajeros, propietarios de vehículos, otros usuarios de la vía pública, etc. Más concretamente, se centra en los datos personales que se tratan dentro del vehículo, que se intercambian entre el vehículo y los dispositivos personales conectados a él (por ejemplo, el teléfono inteligente del usuario) o que se recogen localmente en el vehículo y se exportan a entidades externas (por ejemplo, fabricantes de vehículos, administradores de infraestructuras, compañías de seguros, reparadores de automóviles…) para su tratamiento ulterior[50]. Las Directrices están dirigidas a los fabricantes de vehículos, fabricantes de equipos y proveedores de automóviles, reparadores de automóviles, concesionarios, proveedores de servicios para vehículos, gestores de flotas, compañías de seguros de automóviles, proveedores de entretenimiento, operadores de telecomunicaciones, administradores de infraestructuras viales y autoridades públicas, así como a los interesados[51]. Se trata de una lista no exhaustiva, ya que este ecosistema conlleva una gran variedad de servicios[52].

La *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modi-*

49 Adoptadas por el Comité Europeo de Protección de Datos el 9 de marzo de 2021.

50 Pp. 5 a 9 de las Directrices.

51 El «interesado» es la persona física a la que se refieren los datos objeto del tratamiento. En el contexto de los vehículos conectados, puede ser, en particular, el conductor (principal u ocasional), el pasajero o el propietario del vehículo (pp. 10 a 12 de las Directrices).

52 La mayoría de los datos asociados a los vehículos conectados se considerarán datos personales en la medida en que sea posible vincularlos a una o varias personas identificables. Esto incluye los datos técnicos relativos a los desplazamientos del vehículo (por ejemplo, velocidad, distancia recorrida), así como los relativos al estado del vehículo (por ejemplo, temperatura del refrigerante del motor, revoluciones por minuto del motor, presión de los neumáticos). Permiten deducir el lugar de trabajo y de residencia, así como los centros de interés (ocio) del conductor, y posiblemente revelen información sensible como la religión a través del lugar de culto, o la orientación sexual a través de los lugares visitados, pp. 15 a 18 de las Directrices.

fican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)[53], también conocida como Directiva NIS 2, que debe transponerse a nuestro ordenamiento español, a más tardar, el 17 de octubre de 2024. Entró en vigor en enero de 2023. Sustituye a su predecesora, la Directiva 2016/1148 o Directiva SR1[54], elevando el nivel común de ambición de la UE en materia de ciberseguridad a través de un ámbito de aplicación más amplio, normas más claras y herramientas de supervisión más sólidas, que exigen a los Estados miembros que mejoren sus capacidades de ciberseguridad.

NIS2 es una actualización de la Directiva sobre Seguridad de las Redes y los Sistemas Informáticos (NIS). Al igual que el RGPD, la NIS2 trata de armonizar las medidas y los enfoques en los Estados miembros para proteger la infraestructura digital, en este caso, las mejores prácticas para abordar la creciente avalancha de ciberataques.

Es de destacar su aplicación a los servicios digitales que se ofrecen por las empresas, entre los que se incluyen las redes como servicio, los servidores, los proveedores, los sistemas operativos, la plataforma como servicio, la infraestructura como servicio, el *software* como servicio y servicios dedicados al almacenamiento, tratamiento y transporte de datos, entre otros[55]. Dentro de los sectores que considera de alta criticidad se encuentra el sector del transporte en todas sus modalidades: aéreo, por ferrocarril, marítimo y fluvial y por carretera, y, asimismo, todos los proveedores de infraestructuras digitales[56].

El Gobierno español ha aprobado en el Consejo de ministros del día 14 de enero de 2025, el *Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad*, para transponer la Directiva NIS2, y ofrecer un marco actualizado y sólido para la prevención y gestión de amenazas en el ciberespacio, adaptándose a los crecientes riesgos y cumpliendo con las exigencias de la UE. El Anteproyecto tiene por objeto: reforzar la protección de las redes y sistemas de información; regular un marco institucional y mejorar la coordinación entre autoridades competentes en materia de ciberseguridad; ampliar la cobertura sectorial y garantizar la seguridad jurídica en gestión de riesgos y notificación de incidentes; garantizar un enfoque coherente entre ciberseguridad y seguridad física de las entidades; abordar posibles crisis de ciberseguridad con dimensión exterior o de política común de seguridad y

53 En DOUE de 27-12-2022.

54 *Directiva del Parlamento Europeo y del Consejo relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión* (Directiva NIS). Entró en vigor el 9 de agosto de 2017, en DOUE, 19-7-2016.

55 Véanse los considerandos 33 y 34 de la Directiva.

56 Véase su anexo I.

defensa, y establecer medidas para la gestión de riesgos y obligaciones de notificación de incidentes de ciberseguridad[57].

El Anteproyecto crea el Centro Nacional de Ciberseguridad como la entidad encargada de coordinar las actividades para garantizar un alto nivel de ciberseguridad en España, actuando también como punto de contacto con la UE. El Centro Nacional de Ciberseguridad elaborará la Estrategia Nacional de Ciberseguridad, que establecerá los objetivos estratégicos y las medidas necesarias para mantener un nivel elevado de ciberseguridad.

El *Reglamento 2023/2854 del Parlamento europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento 2017/2394 y la Directiva 2020/1828 (Reglamento de Datos)*[58]*,* que establece un marco armonizado de normas que rigen el acceso, la utilización y puesta a disposición de los datos de los productos conectados y los servicios relacionados, eliminando los obstáculos al buen funcionamiento del mercado interior de datos. Especifica quién tiene derecho a utilizar los datos del producto o del servicio relacionado, en qué condiciones y sobre qué base. Se considera que la proliferación de productos conectados a Internet ha aumentado el volumen y el valor potencial de los datos para los consumidores, las empresas y la sociedad. Los datos interoperables y de alta calidad de diferentes ámbitos incrementan la competitividad y la innovación y garantizan un crecimiento económico sostenible. Habida cuenta de la variedad de productos conectados que producen datos de distinta naturaleza, volumen y frecuencia, que ofrecen oportunidades económicas de diferente valor con el fin de garantizar la coherencia de las prácticas de intercambio de datos en el mercado interior, y de fomentar y promover prácticas justas de intercambio de datos, el Reglamento establece normas horizontales sobre las modalidades de acceso a los datos en aquellos supuestos en que un titular de datos esté obligado por el Derecho de la Unión o por la normativa nacional a poner los datos a disposición de un destinatario de datos. Garantiza que los usuarios de un producto conectado o servicio relacionado en la Unión puedan acceder oportunamente a los datos generados por el uso de dicho producto o servicio y que puedan utilizarlos, entre otros, compartiéndolos con terceros de su elección[59].

El *Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de*

57 ESYS, Empresa, Seguridad y Sociedad Digital, *Anteproyecto de Ley de coordinación y gobernanza de la ciberseguridad,* 16 de enero de 2025, Disponible en https://www.fundacionesys.com/es/el-gobierno-publica-texto-articulado-anteproyecto-ley-de-coordinacion-y-gobernanza-de-la-ciberseguridad/

58 Entró en vigor el 11 de enero de 2024.

59 En DOUE, 22-12-2023.

inteligencia artificial, en el que se reconoce que la ciberseguridad es fundamental para garantizar que los sistemas de inteligencia artificial resistan a las actuaciones de terceros maliciosos que, aprovechando las vulnerabilidades del sistema traten de alterar su uso, comportamiento o funcionamiento, o de poner en peligro sus propiedades de seguridad. Los ciberataques contra sistemas de inteligencia artificial pueden dirigirse contra activos específicos, como los conjuntos de datos de entrenamiento, o los modelos entrenados, o aprovechar las vulnerabilidades de los activos digitales del sistema o la infraestructura de TIC subyacente, por lo que se insta a los proveedores de los sistemas de inteligencia artificial de alto riesgo a adoptar las medidas y los controles de seguridad adecuados[60].

La creciente importancia y el valor de los activos inmateriales en los productos tecnológicos también es reconocido en la reciente *Directiva del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por productos defectuosos*, *y por la que se deroga la Directiva 85/374/CEE del Consejo*, aclarándose que debe también indemnizarse la destrucción o corrupción de datos, incluido el coste de restaurar o de recuperar dichos datos.

Al lado de la normativa comunitaria merece la pena señalar la existencia de unas recomendaciones no vinculantes en esta materia a nivel internacional: la norma ISO/SAE 21434, publicada en agosto de 2021. Es la primera norma internacional para la ciberseguridad en la industria automotriz desarrollada por la Organización Internacional de Normalización juntamente con la Sociedad de Ingenieros Automotrices. Su objetivo es reducir el riesgo de ciberataques incorporando la ciberseguridad en los productos de automoción a lo largo de su vida útil. Las organizaciones son bienvenidas a adoptarla para mejorar sus medidas de ciberseguridad como parte de la diligencia debida, pero no están legalmente obligadas a seguirla. Sin embargo, la norma puede ser un requisito comercial en la cadena de suministro y los fabricantes de vehículos pueden imponer este requisito a los fabricantes de equipo original instalado en el coche, a los desarrolladores de automóviles, a los proveedores de servicios y a otras partes interesadas que participan en el desarrollo de productos[61]. ISO 21434 está diseñado para garantizar que la seguridad cibernética se considere en cada etapa del desarrollo del producto, desde el inicio hasta el retiro. Su objetivo es reducir el riesgo de ciberataques incorporando las buenas prácticas de ciberseguridad en la industria automovilística para organizaciones y profesionales del sector de la automoción[62]. Se ha desa-

60 Véanse el considerando 76 y el art. 15 del mencionado Reglamento.

61 Moldován, C., *Normas de ciberseguridad en la automoción: ISO/SAE 21434 y más,* 19 de septiembre de 2022, Disponible en https://www.endpointprotector.es/blog/normas-de-ciberseguridad-en-la-automocion-iso-sae-21434-y-mas/

62 SGS, *Certificación ISO/SAE 21434 – ingeniería de ciberseguridad para vehículos de carretera,* Disponible en https://www.sgs.com/es-es/services/iso-sae-21434-certificacion-de-vehiculos-de-carretera-ingenieria-de-ciberseguridad

rrollado en paralelo a la regulación obligatoria UNECE WP.29 / R155, con el propósito de proporcionar un marco para garantizar la resiliencia de la ciberseguridad en el diseño, desarrollo, producción, operación, mantenimiento y desmantelamiento de los sistemas eléctricos y electrónicos de los vehículos de carretera. Esto incluye proteger estos sistemas de ataques maliciosos, accesos no autorizados, daños o cualquier otra cosa que pueda interferir con un funcionamiento seguro y protegido.

En España, un paso importante en la protección de la intimidad y de la privacidad en el entorno digital comienza con la *Carta de Derechos Digitales*[63], adoptada por el Gobierno de España el 14 de julio de 2021. Partiendo de que el desarrollo y progresiva generalización de las tecnologías emergentes y de los espacios digitales de comunicación e interrelación que ellas abren, dan lugar a nuevos riesgos, escenarios y conflictos que deben resolverse mediante la adaptación de los valores y derechos constitucionales a este nuevo contexto, consagra el «Derecho a la ciberseguridad», el «Derecho a la protección de datos» y los «Derechos ante la inteligencia artificial». La Carta no trata de crear nuevos derechos fundamentales sino de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros. En consecuencia, la Carta no tiene carácter normativo, sino que su objetivo es reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea, así como sugerir principios y políticas referidas a ellos en el citado contexto. A partir de su publicación, el objetivo es continuar con la difusión y sensibilización sobre sus principios, así como monitorizar e impulsar su integración en la aplicación e interpretación del marco normativo español[64].

Un paso más adelante lo constituye el *Plan Nacional de Ciberseguridad*, aprobado por el Consejo de ministros el 29 de marzo de 2022, con el objetivo de mejorar y de reforzar la ciberseguridad de todo el Estado, y en desarrollo de la Estrategia Nacional de Ciberseguridad 2019. Entre las principales actuaciones destacan: - La creación de la plataforma nacional de notificación y de seguimiento de ciberincidentes y de amenazas que permita intercambiar información en tiempo real entre organismos públicos y privados; - impulsar la puesta en marcha del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y de sus Organismos Públicos; - el desarrollo de un sistema integrado de indicadores de ciberseguridad a nivel nacional; - incrementar la creación de infraestructuras de ciberseguridad en las comunidades y ciudades autónomas y las entidades locales; - impulsar la

63 España Digital 20-26, *Carta de Derechos Digitales,* Disponible en https://espanadigital.gob.es/lineas-de-actuacion/carta-de-derechos-digitales

64 Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital, *Estrategia España Digital 2026*. Disponible en https://portal.mineco.gob.es/es-es/ministerio/estrategias/paginas/00_Espana_Digital.aspx, p. 134.

ciberseguridad de pymes, micropymes y autónomos, y - promover un mayor nivel de cultura de ciberseguridad. Además, el plan prevé la creación de un sistema de seguimiento y control, con el fin de poder identificar el grado de ejecución de las medidas y emitir un informe anual de evaluación[65].

En paralelo y vinculado con el Plan Nacional de Ciberseguridad, se aprueba el *Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación*[66], con el que España transpone las herramientas de la Comisión Europea para el despliegue seguro de las redes 5G en territorio europeo. La norma establece los requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G)[67].

En el terreno concreto de los vehículos autónomos, la UE ha iniciado un avance en la responsabilidad que puede asignarse a los fabricantes de estos vehículos con dos regulaciones emitidas por la Comisión Económica de las Naciones Unidas para Europa, que rigen los requisitos en materia de ciberseguridad que deben cumplir los fabricantes para poder obtener el certificado de conformidad del sistema de gestión de la ciberseguridad. Estas regulaciones, que entrarán en vigor en julio de 2024, son dos Reglamentos: el **R155[68], concerniente a los requisitos para la gestión de la ciberseguridad, y el R156[69], que estipula los requisitos para la gestión de actualizaciones**

---

65 La Moncloa. Referencia del Consejo de Ministros, «Plan Nacional de Ciberseguridad», Nota de prensa, de 29-3-2022. Disponible en https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220329_corregidav02.aspx#ciberseguridad

66 En BOE n.º 76, de 30 de marzo de 2022.
En cumplimiento y desarrollo de esta norma se aprueba el *Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G*, En BOE n.º 106, de 1 de mayo de 2024.

67 El DERECHO.COM. Noticias Jurídicas y Actualidad, «Plan nacional de ciberseguridad», Noticia de prensa de 30-3-2022. Disponible en https://elderecho.com/ciberseguridad-plan-nacional

68 Naciones Unidas, *Reglamento n.º 155 de las Naciones Unidas — Disposiciones uniformes relativas a la homologación de los vehículos de motor en lo que respecta a la ciberseguridad y al sistema de gestión de ésta*, en DOUE, n.º 82, de 9 de marzo de 2021. Entre los posibles efectos de un ataque cibernético, el Reglamento n.º 155 menciona: la afectación del funcionamiento seguro del vehículo; la interrupción del funcionamiento de las funciones del vehículo; la modificación del software y alteración del rendimiento; la alteración del software, la violación de la integridad de los datos; la violación de la confidencialidad de los datos, y la pérdida de disponibilidad de los datos. Véase el Anexo 5 del Reglamento: *Lista de amenazas y sus correspondientes medidas de mitigación.*

69 Naciones Unidas, *Reglamento n.º 156 de las Naciones Unidas – Disposiciones Uniformes relativas a la homologación de vehículos en lo que respecta a las actualizaciones de software y al sistema de gestión de actualizaciones de software,* en DOUE, n.º 82, de 9 de marzo de 2021.

de software. Como he dicho, establecen los requisitos de ciberseguridad que los fabricantes deberán cumplir conforme a la norma ISO/SAE 21434, para optar a la homologación de vehículos que vayan a circular en los países de la UE, o países fuera de la UE que adopten dichos reglamentos[70]. Estas nuevas regulaciones **exigen que todos los vehículos nuevos que se comercialicen en la UE cuenten con medidas de ciberseguridad que sean capaces de proteger contra posibles ataques cibernéticos.**

En España, estos requisitos son de obligado cumplimiento para todos los vehículos a partir del **1 de julio de 2024,** afectando, no solo a los propios vehículos, sino también a la propia operativa de fabricantes y proveedores. El **Instituto Nacional de Ciberseguridad ha adoptado estas normativas y ha comenzado a ofrecer directrices y recursos para ayudar a las empresas del sector automotriz a cumplir con estos nuevos requisitos.** Estas directrices incluyen la evaluación continua de los riesgos y la implementación de tecnologías que permitan la detección y mitigación de amenazas en tiempo real[71]. En este contexto destaca la Asociación Española de Normalización (UNE), entidad legalmente responsable del desarrollo de las normas técnicas, más conocidas como estándares, para la movilidad inteligente y conectada, que ha creado un grupo de expertos de normalización en ciberseguridad IoT, para el desarrollo de estándares internacionales clave de ciberseguridad, que garanticen la seguridad y privacidad en los automóviles autónomos y sistemas de transporte inteligente[72].

Siendo consciente de que los componentes de *hardware* y *software* de los vehículos conectados y automatizados tienen serias repercusiones para la seguridad, la Comisión Europea se ha comprometido a hacer un seguimiento en el futuro de la evaluación en curso de los riesgos de ciberseguridad en los vehículos autónomos conectados con medidas más concretas para hacer frente a los riesgos de ciberseguridad, incluso, si es necesario, en el marco

70 El punto de partida de esta nueva regulación se encuentra en el Foro Mundial para la Armonización de la Reglamentación sobre Vehículos, que pertenece a la Comisión Económica de las Naciones Unidas para Europa (UNECE), que en 2020 aprobó el Reglamento UNECE/TRANS/WP.29/2020/79, que eleva los estándares de ciberseguridad de los vehículos. Este Reglamento entró en vigor el 1 de enero de 2021; CIBERDERECHO, «Ciberseguridad y software para los vehículos: los nuevos cumplimientos entran en vigor el 1 de julio, *Diario La Ley*, 18-6-2024. Disponible en https://diariolaley.laleynext.es/dll/2024/06/19/ciberseguridad-y-software-para-los-vehiculos-los-nuevos-cumplimientos-entran-en-vigor-el-1-de-julio

71 GESPRODAT, «Ciberseguridad en vehículos: Normativas 2024 y su impacto», Nota de prensa. Disponible en https://gesprodat.com/ciberseguridad-en-vehiculos-normativas-2024-y-su-impacto/

72 ESMARTCITY.ES, «La UNE publica un informe sobre normalización en ciberseguridad para la movilidad inteligente», Nota de prensa, de 12-3-2021. Disponible en https://www.esmartcity.es/2021/03/12/une-publica-informe-normalizacion-ciberseguridad-movilidad-inteligente

regulador de los vehículos de motor. Un compromiso de seguir trabajando para lograr una ciberseguridad suficiente sin comprometer la innovación ni la comercialización de estos vehículos[73]. Manifestación de ello es que la UE tiene previsto regular el acceso a los datos de los automóviles mediante una ley específica que tiene por objeto proteger los datos personales de los conductores, de sus vehículos y de sus patrones de movilidad, y permitir que fabricantes, concesionarios, distribuidores y talleres accedan a datos no sensibles. De esta Ley se beneficiarán los conductores que tendrán garantizados sus derechos de protección de datos, y asimismo las aseguradoras, las empresas de leasing y los talleres de reparación, que tendrán un acceso equitativo a los datos de los vehículos. Este proyecto legislativo todavía no aprobado por el Parlamento ni por el Consejo europeo, y que esperemos salga adelante, representa un paso significativo hacia la regulación del creciente mercado de los datos de los vehículos conectados; un sector que promete transformar la industria automotriz y los servicios relacionados[74].

3. Conclusión

En los últimos años las tecnologías innovadoras definidas por software autónomas, junto con la adopción de tecnologías avanzadas del IoT en el ecosistema de la automoción y la movilidad inteligente, han generado una creciente presión regulatoria debido a su mayor vulnerabilidad a los ciberataques. Los actores del sector automotriz se enfrentan al reto de prepararse para nuevas regulaciones, estándares y directrices, así como a la necesidad de desarrollar nuevas prácticas recomendadas en el ámbito de la ciberseguridad. La regulación existente hasta el momento no alcanza a cubrir todos los riesgos, que van en aumento a medida que avanza la tecnología.

Las nuevas tecnologías con IA posibilitan nuevos modos de transporte privados con sus enormes ventajas, pero para conseguir todo ello se necesita ineludiblemente recopilar multitud de datos personales de los ciudadanos, ya que estos sistemas dependen de grandes cantidades de datos para su entrenamiento, aprendizaje y toma de decisiones. De hecho, algunos de los dispositivos basados en IA son recolectores masivos de datos personales

73 «La tecnología de conducción autónoma será un factor determinante para la competitividad y representará una parte significativa del valor añadido futuro. Se espera que genere un valor añadido para el sector automovilístico de hasta 400.000 millones de euros de aquí a 2035»; Comisión Europea*, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de Acción Industrial para el Sector Europeo del Automóvil, op. cit.*

74 Comisión Europea, *Convocatoria de datos para una evaluación de impacto, 2022, Acceso a los datos, las funciones y los recursos del vehículo,* Disponible en https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Acceso-a-los-datos-las-funciones-y-los-recursos-del-vehiculo_es

que se infiltran de manera imperceptible en nuestra vida cotidiana, por lo que no todos los datos que se recogen cuentan con el conocimiento y el consentimiento de los interesados. A esto hay que añadir que los sistemas de IA procesan de manera cada vez más compleja toda esta información personal, consiguiendo resultados a menudo impensables a partir de datos desagregados y muchas veces anónimos. La máquina puede actuar y aprender por medio de una combinación de algoritmos cuya finalidad es asemejarse en todo lo posible a las capacidades del ser humano. Los algoritmos no sólo emplean datos personales de los sujetos, sino que a partir de estos datos se pueden elaborar más volúmenes de datos que aportan una información sobre el individuo totalmente desconocida para este último. Todo lo cual dificulta la aplicación de los principios del RGPD, tal y como fueron configurados en el momento en el que se elaboró, que, ante la llegada de esta nueva tecnología, está empezando a quedarse obsoleto, necesitando de una reconfiguración para adaptarse a las características del funcionamiento de la IA.

El RGPD fue diseñado para los datos personales proporcionados directamente por el interesado, y no para datos inferidos por tecnologías digitales como los sistemas de IA. Una de las posibles soluciones sería actualizar el RGPD para abordar específicamente los desafíos de la IA, con nuevas disposiciones sobre transparencia algorítmica y explicabilidad. También podrían introducirse nuevas reglas para el consentimiento, especialmente en cuanto al uso masivo y reutilización de datos por parte de sistemas de IA.

El Reglamento europeo de Datos de 2023, complementa al RGPD, abriendo la puerta a un nuevo escenario para potenciar la economía digital, mostrando un esfuerzo por equilibrar los derechos de los individuos y las necesidades comerciales. Se centra en el acceso y uso de la información generada por productos y servicios digitales, abriéndose a la posibilidad de nuevos modelos de negocio y más innovación en torno al uso de los datos. Con todo, la práctica demuestra carencias en el caso concreto de la automoción. Todo parece apuntar a que esta Ley de Datos no será suficiente por sí sola para este sector. El ecosistema necesita una legislación específica para el sector automotriz que traduzca los principios y disposiciones de la Ley de Datos en medidas técnicas, legales y concretas. Además, se observa que la ley deja demasiado margen de interpretación, lo que crea inseguridad jurídica y un alto riesgo de litigio.

Este sector necesita de la aprobación urgente de una legislación específica sobre el acceso a los datos de los vehículos. El acceso justo a los datos de los vehículos es esencial para desbloquear todo el potencial de los servicios innovadores beneficiosos para los consumidores y todos los actores del mercado de posventa. No hay más tiempo que perder, ya que la industria del automóvil avanza a un ritmo muy rápido y los proveedores de servicios independientes corren el riesgo de perder su posición competitiva.

La industria automotriz se enfrentará a mayores desafíos de ciberseguridad impulsados por la proliferación de vehículos conectados y autónomos.

Para afrontar este panorama en constante evolución, las partes involucradas deben adoptar marcos de ciberseguridad robustos, realizar evaluaciones rigurosas de proveedores e implementar estrategias proactivas de detección de amenazas.

La IA puede ocupar un lugar central en la lucha contra estos riesgos. La integración de IA en los procesos de detección, investigación y mitigación puede permitir una detección más rápida de anomalías, una identificación más precisa de amenazas y respuestas rápidas y automatizadas, estableciendo un nuevo estándar de protección en el ecosistema de la movilidad. Los avances en IA pueden mejorar la protección de datos y la privacidad mediante el desarrollo de tecnologías de encriptación más avanzadas y sistemas de anonimización de datos y algoritmos de detección de brechas de seguridad. Estas tecnologías podrían ayudar a minimizar los riesgos de exposición de datos personales y asegurar el cumplimiento del principio de minimización de datos del RGPD. Como ya ha sucedido con otras tecnologías, de cara a la protección de datos o a la ciberseguridad implican un arma de doble filo: de un lado exponen y ponen en peligro esta información o datos o abren posibles brechas, pero al mismo tiempo pueden ser unas buenas herramientas para luchar automatizadamente contra estos peligros.

Desde el punto de vista de la normalización y la estandarización, queda mucho trabajo por hacer en materia de seguridad y privacidad dentro del ámbito de la industria de la movilidad conectada y automatizada. Constituye un gran reto el diseñar y consensuar los estándares técnicos que permitan encontrar un equilibrio entre la privacidad y el desarrollo tecnológico.

4. Bibliografía

ANFAC, *Informe Vehículo Autónomo y Conectado,* 2023, p. 28.

B. Fernández, C, «Contenido de la propuesta de Reglamento europeo sobre privacidad de las comunicaciones electrónicas», *Diario La Ley*, Wolters Kluwer, 3-5-2017.

CIBER PROTEGIDOS, «El impacto de los coches autónomos en las estrategias de ciberseguridad».

CIBERDERECHO, «Ciberseguridad y software para los vehículos: los nuevos cumplimientos entran en vigor el 1 de julio, *Diario La Ley*, 18-6-2024.

CIBERSEGURIDAD, «Ciberseguridad en vehículos conectados y autónomos», *Nota de prensa*, 2024.

Comisión Europea, «Liberar el potencial de los datos de movilidad», *Nota de prensa*, 19-septiembre-2024.

Comisión Europea, Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Plan de Acción Industrial para el Sector Europeo del Automóvil (COM/2025/95 final), Bruselas, 5 de marzo de 2025.

Comisión Europea, *Convocatoria de datos para una evaluación de impacto, 2022, Acceso a los datos, las funciones y los recursos del vehículo.*

Dirección General de Tráfico, «Vehículos de conducción automatizada. Los vehículos de conducción automatizada representan una revolución para la movilidad del futuro», *Nota de prensa*, 21 de marzo de 2024.

ECIJA, *Directrices 2/2023 sobre el alcance técnico del art. 5.3 de la Directiva ePrivacy,* Nota de prensa de 19-12-2024.

EL DERECHO.COM, «Plan nacional de ciberseguridad», *Noticias Jurídicas y Actualidad,* Noticia de prensa de 30-3-2022.

ENISA (Agencia de la Unión Europea para la Ciberseguridad), *Guía de prácticas para para la seguridad de los coches inteligentes***,** 2019.

ESMARTCITY.ES, «La UNE publica un informe sobre normalización en ciberseguridad para la movilidad inteligente», *Nota de prensa* de 12-3-2021.

España Digital 20-26, *Carta de Derechos Digitales.*

España Pérez, J.A, «La problemática jurídica de la protección de datos en la Smart mobility. Especial referencia al Reglamento 2016/679», *Revista española de Derecho Administrativo* 207, julio-septiembre, 2020.

ESYS, EMPRESA, SEGURIDAD Y SOCIEDAD DIGITAL, *Anteproyecto de Ley de coordinación y gobernanza de la ciberseguridad,* 16 de enero de 2025.

Fernández, A, «Crecen los ciberataques a coches eléctricos y conectados», *Coche global*, Noticia de prensa, 2 de marzo de 2025.

Fernández, J. A, «El Reglamento (RGPD) y la inteligencia artificial», en *Seifti,* Nota de prensa de 12 de febrero de 2024.

Fundación Capgemini, *Libro Blanco para un vehículo autónomo inclusivo,* 2025.

GESPRODAT, «Ciberseguridad en vehículos: Normativas 2024 y su impacto», *Nota de prensa de 21-8-2024*.

Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital, *Estrategia España Digital 2026*.

González Prieto, A, *Ciberseguridad en vehículos conectados y autónomos: estudio de las comunicaciones V2X*. Dir. por Jordi Serra Ruiz, Máster Universitario en Ciberseguridad y Privacidad, Universitat Oberta de Catalunya, 2022.

Grupo Adaptalia, *Reglamento ePrivacy: qué es y cómo impacta en la privacidad online,* Nota de prensa de 14-3-2025.

Grupo Atico34, «Protección de Datos e Inteligencia Artificial», *Nota de prensa* 2024.

Hackrisk, «La ciberseguridad en vehículos autónomos: retos y soluciones para un futuro seguro», *Nota de prensa 2024*.

Historia de la Tecnología, «La ciberseguridad en los vehículos autónomos: desafíos y soluciones», *Nota de prensa 2024*.

ITC Web Solutions, «La ciberseguridad en vehículos autónomos: riesgos y soluciones», *Nota de prensa*, 2024.

JOSESILVA. Correduría de Seguros, «La ciberseguridad de los vehículos conectados», 2023.

LA LEY WOLTERS KLUWER, «Publicado el Reglamento sobre ciberseguridad de la Unión Europea», *Diario La Ley*, 10-6-2019.

La Moncloa. Referencia del Consejo de Ministros, «Plan Nacional de Ciberseguridad», *Nota de prensa*, de 29-3-2022.

López-Lapuente, L, «La nueva regulación europea de los datos: cómo dar forma al futuro digital de Europa», *Actualidad Jurídica Uría Menéndez,* n.º 61, 2023.

Lubomira Kubica, M, «Vehículos autónomos y la privacidad: una perspectiva norteamericana», en Sancho López y Martínez Velencoso, *Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación*, Aranzadi, 2022.

Moldován, C, *Normas de ciberseguridad en la automoción: ISO/SAE 21434 y más,* 19 de septiembre de 2022.

Naciones Unidas, *Reglamento n.º 155 de las Naciones Unidas — Disposiciones uniformes relativas a la homologación de los vehículos de motor en lo que respecta a la ciberseguridad y al sistema de gestión de ésta*, en DOUE, n.º 82, de 9 de marzo de 2021.

Naciones Unidas, *Reglamento n.º 156 de las Naciones Unidas – Disposiciones Uniformes relativas a la homologación de vehículos en lo que respecta a las actualizaciones de software y al sistema de gestión de actualizaciones de software,* en DOUE, n.º 82, de 9 de marzo de 2021.

Parlamento Europeo, *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),* en DOUE, 4-5-2016.

Parlamento Europeo, *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 («Reglamento sobre la Ciberseguridad»)*, en DOUE n.º 151, de 7 de junio de 2019.

Parlamento Europeo, *Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC),* en DOUE n.º 482, de 7 de febrero de 2024.

Parlamento Europeo, *Propuesta de reglamento del parlamento europeo y del consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)*, Bruselas, 10-1-2017.

Porras, O., «Ciberseguridad para vehículos: transporte, conectividad, conceptos y especificaciones tecnológicas», 2025.

Redondo Martín, J.A., «Qué es Big Data: Funcionamiento, Aplicaciones y Salidas Profesionales», *CEU*, 2025.

Rubí Puig, A., «Inteligencia artificial y daños indemnizables», Capítulo XI, en Álvarez Lata, N, *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*, Aranzadi, 2024.

S2GRUPO, *Segundo informe de ciberseguridad en vehículos eléctricos conectados 2025*, 12-marzo-2025.

SAP, «¿Qué es internet de las cosas (IoT)?», Nota de prensa de 20-enero-2023.

SGS, *Certificación ISO/SAE 21434 – ingeniería de ciberseguridad para vehículos de carretera.*

SOFTWARE, «Inteligencia artificial y protección de datos: cómo afecta el RGPD?», *Noticia de prensa* de 25-10–2024.

UNE (Normalización Española), «Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno», 2021.

UPSTREAM, *Informe de ciberseguridad global sobre movilidad inteligente y automotriz 2025*.