**TEMÁTICA: INTERACCIÓN DE LA IA Y LA PROTECCIÓN DE DATOS EN EL DERECHO**

**TÍTULO DE LA COMUNICACIÓN:**

***LA IMPORTANCIA DE LA CIBERSEGURIDAD EN***

***LOS VEHÍCULOS AUTÓNOMOS Y SU PROTECCIÓN EN LA***

***LEGISLACIÓN EUROPEA***

RESUMEN DE LA COMUNICACIÓN

Esta comunicación tiene por objeto resaltar la importancia de la ciberseguridad en los vehículos autónomos dotados con inteligencia artificial que funcionan sin conductor y la protección jurídica brindada hasta la fecha por las instancias europeas[[1]](#footnote-1).

Un tipo de daño que es característico en la utilización de los vehículos autónomos conectados (CAV) es el que deriva de los ciberataques al vehículo, que pueden ocasionar daños tanto al propio usuario como a terceros.  Los CAV son plataformas tecnológicas complejas que dependen de sensores, sistemas de comunicación, redes y datos. Esta conectividad masiva los convierte en objetivos atractivos para los ciberdelincuentes. La dependencia de tecnologías avanzadas hace que la ciberseguridad sea un componente crítico para garantizar la seguridad de los usuarios, de los peatones y de las infraestructuras conectadas.

Los CAV dependen de la comunicación “vehículo a todo” para interactuar con otros coches, infraestructuras, redes y peatones. Es decir, tienen los siguientes tipos de comunicaciones vehiculares: de vehículo a vehículo[[2]](#footnote-2), de vehículo a infraestructura[[3]](#footnote-3), de vehículo a peatón[[4]](#footnote-4) y de vehículo a red[[5]](#footnote-5). Un pirata informático, mediante el secuestro remoto, puede tomar el control total del automóvil[[6]](#footnote-6), pudiendo, por ejemplo, causar colisiones o interrumpir el tráfico, originar un comportamiento impredecible del vehículo, o interferir en la dirección, el frenado o la aceleración[[7]](#footnote-7).

Los CAV producen y almacenan datos nuevos cada segundo y utilizan la computación en la nube para un almacenamiento y recuperación rápidos. Si un hacker pudiera acceder a la base de datos en la nube de un automóvil, podría manipular muchas funciones de éste, como activar o desactivar los frenos, el volante o aumentar la velocidad del vehículo[[8]](#footnote-8). Los investigadores ya han demostrado que los vehículos inteligentes e informatizados pueden ser secuestrados con sólo un ordenador portátil, un hardware de bajo coste o un software fácil de obtener. Los piratas informáticos ya han demostrado que pueden controlar a distancia la dirección, e incluso desactivar los frenos y apagar el motor a distancia cuando el vehículo está en movimiento[[9]](#footnote-9).

A ello se le suma otra vulnerabilidad, y es que recopilan una gran cantidad de información personal de los usuarios y pasajeros, como la ubicación, los hábitos de conducción y las preferencias de entretenimiento. Esta información puede ser muy valiosa para los hackers, ya que puede ser utilizada para actividades fraudulentas o para violar la privacidad de los usuarios[[10]](#footnote-10). 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 si dichos datos pasan por sus sistemas de información. 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[[11]](#footnote-11).

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[[12]](#footnote-12), y 2) el hacker puede acceder a la información personal de los usuarios[[13]](#footnote-13).

Desde la Unión Europea (UE) se está potenciando el desarrollo de los CAV por los muchos beneficios que aportarán, pero al mismo tiempo, siendo consciente de estos peligros que comportan se han presentado iniciativas que reconocen la creciente importancia de la protección de los datos personales y de la privacidad. Por su incidencia en los vehículos autónomos deben resaltarse las siguientes:

Las *Directrices 1/2020, sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad*[[14]](#footnote-14), 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 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 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[[15]](#footnote-15).

La *Directiva 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 modifican el Reglamento 910/2014 y la Directiva 2018/1972 y por la que se deroga la Directiva 2016/1148 (Directiva SRI 2)[[16]](#footnote-16)*, que debe transponerse a nuestro ordenamiento español, a más tardar, el 17 de octubre de 2024. Establece las medidas y obligaciones que los Estados miembros deben adoptar al objeto de alcanzar un elevado nivel común de ciberseguridad[[17]](#footnote-17).

Dentro de los sectores que considera de alta criticidad se encuentra el sector del transporte en todas sus modalidades y, asimismo, todos los proveedores de infraestructuras digitales[[18]](#footnote-18).

La creciente importancia y valor de los activos inmateriales en los productos tecnológicos ha sido reconocida asimismo en la nueva la nueva *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*[[19]](#footnote-19), aclarándose que debe indemnizarse la destrucción o corrupción de datos, incluido el coste de restaurar o recuperar dichos datos[[20]](#footnote-20).

La mencionada Directiva ha sido complementada con el *Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia*)[[21]](#footnote-21), que tiene por objeto el establecimiento de un marco jurídico uniforme relativo a los requisitos esenciales de ciberseguridad para la introducción de productos con elementos digitales en el mercado de la Unión. Se considera que, aunque el Derecho vigente de la Unión se aplica a determinados productos con elementos digitales, no existe un marco regulador horizontal que establezca requisitos de ciberseguridad exhaustivos para todos los productos con elementos digitales. Los diversos actos e iniciativas adoptados hasta la fecha a escala de la Unión abordan solo de manera parcial los problemas y riesgos detectados en relación con la ciberseguridad, creando un mosaico legislativo dentro del mercado interior, aumentando la inseguridad jurídica tanto para los fabricantes como para los usuarios de dichos productos[[22]](#footnote-22). El Reglamento cataloga las vulnerabilidades[[23]](#footnote-23)de ciberseguridad como un defecto de fabricación imputable al fabricante. Cuando dicha falta de seguridad consista en una falta de las actualizaciones necesarias posteriores a la introducción del producto en el mercado y ésta cause daños, se aplicará igualmente la responsabilidad del fabricante. Además de las obligaciones dirigidas a los fabricantes y demás operadores, el Reglamento contempla una información e instrucciones para los usuarios dirigidas a garantizar la seguridad de éstos y un uso seguro de los productos[[24]](#footnote-24).

En el terreno concreto de los vehículos autónomos, la UE ha dado un paso más adelante en la responsabilidad que puede asignarse a los fabricantes de estos vehículos con dos nuevas 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 de gestión de la ciberseguridad. Estas regulaciones son dos Reglamentos: el **R155**[[25]](#footnote-25)**, concerniente a los requisitos para la gestión de la ciberseguridad*,* y el R156**[[26]](#footnote-26)**, que estipula los requisitos para la gestión de actualizaciones de *software***[[27]](#footnote-27).

En España, estos requisitos son de obligado cumplimiento para todos los vehículos a partir del **1 de julio de 2024**. E**l 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**[[28]](#footnote-28)**.**

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, financiado por el Ministerio de Ciencia e Innovación, que lleva por título: *Conducción autónoma y seguridad jurídica del transporte*. IP. Eliseo Sierra Noguero. [↑](#footnote-ref-1)
2. Intercambio de información en tiempo real entre vehículos que se encuentren próximos. Generalmente, se transmite y recibe información relativa a la velocidad del vehículo, su rumbo o intención. Cada vehículo constituye un nodo de la red que puede recibir información y retransmitirla; GONZÁLEZ PRIETO, Alexander, *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. [↑](#footnote-ref-2)
3. 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, Alexander, op.cit. p.20. [↑](#footnote-ref-3)
4. 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, Alexander, op.cit. p.20. [↑](#footnote-ref-4)
5. El tipo de información recibida puede ser de varios tipos, desde información meteorológica, hasta información sobre el estado del tráfico, rutas alternativas, etc; GONZÁLEZ PRIETO, Alexander, op.cit. p.20. [↑](#footnote-ref-5)
6. “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/> [↑](#footnote-ref-6)
7. 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> [↑](#footnote-ref-7)
8. CIBERSEGURIDAD, “Ciberseguridad en vehículos conectados y autónomos”, Nota de prensa, 2024, Disponible en <https://ciberseguridad.com/guias/industrial/vehiculos-conectados-autonomos/> [↑](#footnote-ref-8)
9. UNE (Normalización Española), *Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno,* 2021, p.5, Disponible en <https://revista.une.org/37/normalizacion-en-ciberseguridad-para-la-movilidad-inteligent.html> [↑](#footnote-ref-9)
10. 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/> [↑](#footnote-ref-10)
11. UNE (Normalización Española), *Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno*, op.cit, p.5 [↑](#footnote-ref-11)
12. Poniendo en peligro la vida de los ocupantes del vehículo o de terceros. [↑](#footnote-ref-12)
13. Provocando una vulneración de la intimidad del propietario o usuario del vehículo. [↑](#footnote-ref-13)
14. Adoptadas por el Comité Europeo de Protección de Datos el 9 de marzo de 2021. [↑](#footnote-ref-14)
15. Páginas 5 a 9 de las Directrices. [↑](#footnote-ref-15)
16. En DOUE de 27-12-2022. [↑](#footnote-ref-16)
17. Véanse los considerandos 33 y 34 de la Directiva. [↑](#footnote-ref-17)
18. Véase su anexo I. [↑](#footnote-ref-18)
19. DOUE, núm. 2853, de 18 de noviembre de 2024. [↑](#footnote-ref-19)
20. Véase el considerando 20 de la Directiva. [↑](#footnote-ref-20)
21. En DOUE núm. 2847, de 20 de noviembre de 2024. [↑](#footnote-ref-21)
22. Contenidas en el Anexo II del Reglamento. [↑](#footnote-ref-22)
23. En su art. 3 apart.40, define la “vulnerabilidad”, como la deficiencia, susceptibilidad o fallo de un producto con elementos digitales que puede ser aprovechada por una ciber amenaza. Es decir, una vulnerabilidad que puede ser utilizada de manera efectiva por un agente malintencionado en condiciones operativas prácticas (apart.41). [↑](#footnote-ref-23)
24. Contenidas en el Anexo II del Reglamento. [↑](#footnote-ref-24)
25. *Reglamento Nº. 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, núm. 82, de 9 de marzo de 2021. [↑](#footnote-ref-25)
26. *Reglamento Nº. 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, núm.82, de 9 de marzo de 2021. [↑](#footnote-ref-26)
27. 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 entra en vigor a partir del 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> [↑](#footnote-ref-27)
28. En 2021 publicó el *Informe Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno,* elaborado con la colaboración de las organizaciones participantes del Grupo Específico CTN320/GT CAV “Ciberseguridad en Ámbito del Vehículo” del CTN 320 de UNE. El objetivo del informe, coordinado por el Colegio Oficial de Ingenieros Técnicos de Telecomunicación, es anticiparse al desarrollo previsto en los sistemas cooperativos inteligentes de transporte y en los avances en la conectividad del vehículo con el entorno. Además, pretende preparar los estándares técnicos que permitan tanto ofrecer la interoperabilidad necesaria de todos los elementos de estos grandes sistemas de transporte, como estandarizar los requisitos de seguridad y privacidad necesarios para dotarlos de las garantías suficientes. El documento analiza los avances que se están desarrollando actualmente en el campo de las normas y reglamentos a nivel gubernamental y de los diferentes agentes del sector. También identifica los órganos técnicos de normalización, estándares e iniciativas relevantes relativos a la ciberseguridad y la privacidad en el ámbito general de la industria de la Movilidad Conectada y Automatizada y en el caso particular de los Vehículos Conectados y Autónomos, los Sistemas Inteligentes de Transporte y las tecnologías de comunicación y conectividad involucradas. El informe señala la necesidad de contar con nuevas normas técnicas en el ámbito de la industria de la CAM para dar respuesta a los riesgos de ciberseguridad y privacidad que conllevan los avances tecnológicos en este ámbito. En este sentido, el documento pretende servir de base para el desarrollo de futuras iniciativas en el campo de la normalización en ciberseguridad y privacidad de la movilidad inteligente y los vehículos conectados, aunando y consensuando los esfuerzos de expertos y empresas con el objetivo de crear un entorno confiable; ESMARTCITY.ES. TODO SOBRE CIUDADES INTELIGENTES, “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> [↑](#footnote-ref-28)