Cuando el atentado no necesita atacante: la nueva frontera de la reconstrucción de siniestros

Por Santiago Navas, Forentia360

Durante años, la reconstrucción técnica de un siniestro de tráfico se ha apoyado en certezas relativamente sólidas: física de impacto, tiempos de reacción humana, huellas de frenada, trazas mecánicas. Cuando algo fallaba en un vehículo —unos frenos manipulados, una dirección forzada—, esa manipulación dejaba rastro. Un perito con buena formación podía, tarde o temprano, reconstruir la cadena causal. Esa certeza está dejando de ser absoluta y conviene decirlo con claridad antes de que la realidad nos adelante.

Imagen generada con IA

Una amenaza que ya no es ciencia ficción

Un Trabajo de Fin de Máster del Centro Universitario de la Guardia Civil (CUGC), calificado con sobresaliente y mención especial del tribunal, analiza con metodología contrastada cómo el terrorismo yihadista podría secuestrar la tecnología de conducción autónoma para sembrar el terror en lugares de aglomeración. El trabajo lo firma el teniente coronel Cristóbal Fattizzo Padilla, dentro del Máster Oficial Universitario en Inteligencia y Contraterrorismo del CUGC, bajo la dirección académica del abogado y doctor José María Fuster-Fabra Torrellas, socio decano de Fuster-Fabra Abogados.

El estudio parte de una realidad ya consolidada en Europa: el vehículo como arma, con precedentes en Niza, Berlín, Londres y Barcelona. La pregunta que plantea la investigación es inquietante en su simplicidad: ¿qué ocurre cuando ese vehículo ya no necesita conductor? La conducción autónoma avanza en España con vocación de liderazgo europeo y esa misma tecnología abre un escenario que organismos como Naciones Unidas y Europol ya contemplan: la posibilidad de ejecutar un atentado sin que el atacante esté físicamente en el coche. Sin conductor identificable. Sin presencia física que neutralizar in situ.

Para sostener su análisis, el autor recurre a marcos de gestión del riesgo como las normas ISO 31000 e ISO 31010 y a la guía ProtectUK del Centro Nacional de Contraterrorismo del Reino Unido y propone crear en la Guardia Civil unidades especializadas en detección y neutralización de este vector, siguiendo el modelo de las unidades C-UAS antidrones que el Cuerpo ya despliega en grandes eventos.

De la pericia mecánica a la pericia digital

Desde la criminología aplicada a la siniestralidad vial llevamos tiempo señalando que el campo de la reconstrucción ya no puede limitarse a la física clásica y los tiempos de reacción del conductor. Esa limitación tenía sentido cuando el vehículo era, en esencia, un sistema mecánico gobernado por un humano. Hoy el vehículo es, cada vez más, un sistema informático sobre ruedas y eso cambia radicalmente qué hay que buscar cuando algo sale mal.

Una manipulación de frenos era —y sigue siendo, en vehículos convencionales— una cuestión mecánica: discos, latiguillos, líquido de frenos, elementos físicos que un perito puede inspeccionar, fotografiar y datar. Pero en un vehículo con sistemas ADAS avanzados, conectividad V2X o capacidades de conducción autónoma, esa misma manipulación puede no dejar ninguna huella material. Puede ser una orden ejecutada por software, un comando inyectado en una red CAN, una instrucción remota camuflada entre millones de "1" y "0" que el sistema interpreta como legítima. No hay metal doblado que examinar; hay que examinar código, registros y arquitecturas de seguridad que la mayoría de los operadores jurídicos —y muchos peritos— todavía no dominan.

Esto no es un escenario aislado. Conecta directamente con cuestiones que ya hemos abordado en otros análisis: la vulnerabilidad de los sistemas ADAS regulados por el Reglamento (UE) 2019/2144, los riesgos de manipulación en infraestructuras de carga de vehículos eléctricos, o las debilidades de los sistemas de balizamiento BLE. Todos comparten un mismo denominador: la superficie de ataque ya no es solo física, es digital y las herramientas tradicionales de reconstrucción de siniestros no están preparadas para auditarla.

El respaldo que llega desde Bruselas

Lo llamativo es que esta hipótesis, lejos de ser un ejercicio académico aislado, queda corroborada casi al mismo tiempo por un documento de enorme peso institucional: la Evaluación Coordinada de Riesgos de la UE sobre Vehículos Conectados y Automatizados (CAV), publicada el 30 de enero de 2026 por el Grupo de Cooperación NIS, en colaboración con la Comisión Europea y ENISA, al amparo del artículo 22 de la Directiva NIS2.

El informe es contundente. Los Estados miembros, la Comisión y ENISA identificaron y evaluaron 107 riesgos asociados a los vehículos conectados y automatizados, de los cuales 14 fueron calificados como riesgos prioritarios. Y entre las conclusiones más inquietantes está esta: los CAV procesan grandes volúmenes de datos personales y sensibles, lo que los convierte en objetivos o vectores potenciales de vigilancia y espionaje e incluso podría permitir su uso como arma.

El documento no se queda en la advertencia genérica. Entre los riesgos prioritarios identificados figura el escenario en que un país hostil presiona a un fabricante de CAV que opera en su jurisdicción para implementar hardware o software oculto y malicioso, actualizaciones o configuraciones en sus productos con el fin de manipular físicamente la flota y el escenario equivalente dirigido a un proveedor de primer nivel (fabricantes de unidades de control electrónico, proveedores de nube, fabricantes de sensores). Es, en esencia, el mismo vector que plantea el TFM del CUGC, descrito ahora con el lenguaje técnico de un organismo regulador europeo.

Más relevante todavía para quienes trabajamos en reconstrucción de siniestros: los expertos consultados identificaron como riesgo prioritario que un país hostil altere el funcionamiento de los sistemas de conducción automatizada en la fase de entrenamiento, provocando comportamientos inesperados en situaciones específicas en el extranjero —por ejemplo, interpretando peligrosamente la situación de la vía o siendo utilizado como arma en un momento concreto o tras una orden específica. No es ciencia ficción: es, literalmente, un riesgo catalogado, evaluado y priorizado por el regulador europeo.

El informe documenta además que la base técnica de estos escenarios ya ha sido demostrada en la práctica. Investigadores lograron en 2015 la manipulación remota de la transmisión, la dirección y el frenado de un vehículo sin alterar el coche ni necesitar interacción física —un hallazgo que provocó la retirada de 1,4 millones de vehículos por parte del fabricante afectado—. En 2016 se demostró un ataque remoto que comprometía el bus CAN del vehículo y permitía el control de las funciones de conducción. Y en 2023, investigadores lograron una cadena completa de ataque remoto hasta el bus CAN en un modelo de vehículo popular, partiendo de Bluetooth, pasando por el chip inalámbrico y el núcleo Linux, hasta sortear la pasarela de seguridad.

El informe añade un matiz que conviene subrayar: estos riesgos no son hipotéticos en cuanto a la capacidad técnica subyacente. En 2022, un conocido fabricante de tractores deshabilitó remotamente sus propios vehículos sustraídos en el contexto de la guerra en Ucrania —una capacidad de inmovilización remota que numerosos fabricantes de automóviles también incorporan, normalmente como servicio antirrobo—. La existencia de estas vías de control remoto está bien

documentada; lo que cambia es la confianza en que un proveedor de alto riesgo, sujeto a presión militar o gubernamental en su país de origen, no las active en otro sentido. El régimen de homologación de tipo —concluye el informe— fue creado principalmente para garantizar la seguridad vial y no mitiga suficientemente este tipo de riesgo cuando proviene de la coacción a un proveedor.

Infraestructura de carga: el eslabón más débil

El informe europeo añade un matiz que conecta directamente con nuestro análisis previo sobre vehículos eléctricos y ciberataques en garajes comunitarios: la infraestructura de carga está peor protegida de lo que cabría esperar. Un estudio reciente de 235 sistemas de carga rápida en corriente continua desplegados públicamente en cuatro países europeos mostró que solo el 12% de las estaciones analizadas implementaba seguridad de capa de transporte (TLS), dejando al resto vulnerable a ataques demostrados desde hace años. El riesgo prioritario identificado en este ámbito es directo: un atacante que se dirige al sistema de carga provocando la sobrecarga del sistema de almacenamiento de energía recargable, con el consiguiente exceso de calor y riesgo de explosión —exactamente el fenómeno de "thermal runaway" que ya habíamos señalado como riesgo en garajes comunitarios.

Implicaciones para la pericia judicial

Si el TFM del CUGC y el informe de la UE coinciden —y lo hacen, con notable precisión—, el sistema judicial y pericial español se enfrenta a varios retos inmediatos:

- **Formación pericial híbrida.** Los peritos de siniestros viales necesitarán nociones de ciberseguridad automotriz, no solo de física del impacto.
- **Cadena de custodia digital.** Los registros de telemetría y firmwares deberán tratarse con el mismo rigor que hoy se aplica a una caja negra de aviación.

- **Atención al proveedor, no solo al fabricante.** El informe de la UE subraya que estas preocupaciones no se aplican exclusivamente a vehículos completos fabricados por proveedores de alto riesgo, sino también a componentes individuales, en la medida en que pueden usarse como vector de ataque. La pericia tendrá que mirar más allá de la marca del coche.
- **Cooperación con unidades especializadas.** La propuesta del CUGC de crear unidades específicas, en la línea de las C-UAS antidrones, debería complementarse con protocolos de colaboración entre esas unidades y los peritos judiciales que finalmente tendrán que explicar los hechos ante un tribunal.
- **Marco normativo.** Los propios autores del informe europeo reconocen que los riesgos derivados de proveedores de alto riesgo están actualmente insuficientemente abordados por el marco regulador vigente. La responsabilidad penal y civil en estos escenarios —fabricante, operador de flota, proveedor de software, atacante— exige un desarrollo normativo que hoy es, en el mejor de los casos, incipiente.

Ver la amenaza antes de que ocurra

El director académico del TFM resumió el espíritu del trabajo señalando que su autor tuvo la capacidad de ver una amenaza que aún no ha ocurrido y de argumentar por qué hay que estar preparados antes de que ocurra. El informe de la UE, publicado apenas unos meses antes, confirma que esa capacidad de anticipación no es exclusiva de un trabajo académico: es ya una prioridad reconocida al más alto nivel institucional europeo, con 107 riesgos catalogados y 14 calificados como críticos y con un Grupo de Cooperación NIS que recomienda expresamente a la Comisión y a los Estados miembros reducir la dependencia de proveedores de alto riesgo en los sistemas más sensibles del vehículo: procesamiento y toma de decisiones, comunicación y conectividad y control del vehículo.

No se trata de demonizar la conducción autónoma ni los avances tecnológicos del sector. Se trata de reconocer, con la misma honestidad con la que reconocemos

sus beneficios en seguridad vial, que toda tecnología que permite controlar un vehículo sin intervención humana directa es, por definición, una tecnología que puede ser secuestrada por quien quiera hacer daño. El problema nunca ha sido la tecnología. El problema, como siempre, son las mentes criminales —o los Estados hostiles— dispuestos a ponerla al servicio del terror.

Fuentes:

Confilegal, "Un coche que mata sin nadie al volante: un TFM premiado por la Guardia Civil anticipa el yihadismo de los vehículos autónomos", 20/06/2026 (Enrique de la Llave)

NIS Cooperation Group, en cooperación con la Comisión Europea y ENISA, "Connected and Automated Vehicles — EU Coordinated Risk Assessment", 30/01/2026, elaborado conforme al artículo 22 de la Directiva (UE) 2022/2555 (NIS2).