

DULCINEA DEL TRUE CRIME II — EXPEDIENTE ÓRBITA

Del coche que nadie había hackeado, hasta que alguien lo hizo, y de cómo un taller dejó la puerta abierta sin saberlo

Nuevos casos, mismas personas

El accidente de Felisa Roldán no tenía sentido, y eso fue, paradójicamente, lo único que durante las primeras semanas nadie quiso escuchar.

Felisa tenía cincuenta y ocho años, vivía en Tomelloso, a media hora de Olmeda del Espino y conducía un sedán de gama media de los llamados *coches conectados*: con conectividad permanente a internet, actualizaciones de software, asistentes de conducción y una aplicación móvil que permitía, entre otras cosas, localizar el vehículo, abrir las puertas a distancia y, en teoría, recibir alertas si algo iba mal con el motor.

Un martes de septiembre, circulando por la autovía a unos noventa kilómetros por hora, el volante de Felisa giró solo.

No fue brusco. No fue violento. Fue, según describiría ella después con una precisión que la propia policía encontró difícil de catalogar, *"como si alguien hubiera puesto las manos sobre las mías y las hubiera movido con suavidad hacia la derecha"*. El coche se desvió hacia el carril contiguo. Felisa, con un reflejo que probablemente le salvó la vida, contrarrestó el giro con fuerza. El coche volvió a su carril, dio un bandazo y acabó parado en el arcén con dos ruedas reventadas; y Felisa, con el cuello dolorido durante tres semanas y un susto que no se le pasó en mucho más tiempo.

Cuando Felisa contó lo que había pasado —al seguro, a la Guardia Civil de Tráfico, a su familia—, la respuesta fue, en todos los casos, una variante educada de lo mismo: los coches modernos tienen sistemas de asistencia que a veces corrigen la trayectoria de forma que puede sentirse extraña; probablemente el sistema de mantenimiento de carril había interpretado mal una línea desgastada del asfalto; los neumáticos, ya se sabe, con el calor de septiembre y el desgaste.

Felisa decía que no. Que ella conocía su coche, que llevaba dos años conduciéndolo, que sabía perfectamente cómo se sentía el asistente de mantenimiento de carril cuando corregía la trayectoria —un tirón breve, perceptible, que avisaba— y que esto había sido otra cosa. Más suave. Más sostenido. Y, sobre todo, dirigido: el volante no había vibrado ni avisado. Simplemente había girado, como si lo hiciera otra persona.

Nadie la creyó. Hasta que pasó una segunda vez.



De la segunda vez y de la llamada a la asociación

La segunda vez ocurrió tres semanas después, en una calle del pueblo, a quince kilómetros por hora. Felisa estaba aparcando. El coche, en mitad de la maniobra, giró el volante hacia el lado contrario al que ella había puesto, golpeando suavemente el bordillo. Sin consecuencias, esta vez. Pero Felisa, que ya no estaba dispuesta a que le dijeran que eran los neumáticos, llevó el coche al concesionario oficial de la marca y exigió una revisión completa del sistema electrónico.

El concesionario no encontró nada. *"Todo dentro de parámetros"*, decía el informe. Felisa, frustrada, mencionó el caso —de pasada, en una conversación sobre seguros— a una compañera de trabajo cuya hermana, según le había contado alguna vez, asistía a una asociación de víctimas de tráfico en Olmeda del Espino donde, decía la hermana, *"había un hombre mayor que sabía mucho de estas cosas y otra persona, una criminóloga, que también ayudaba"*.

La compañera le dio el contacto. Felisa, sin mucha fe, escribió un correo.

Don Justo lo leyó un martes, después de la reunión. Lo leyó dos veces. Y por primera vez en mucho tiempo sintió algo que no era exactamente la vieja excitación de las furgonetas y los mapas, pero que se le parecía lo suficiente como para que tuviera que pararse un momento a distinguirlo.

La diferencia, esta vez, era que no actuó solo.



De la llamada a tres bandas

Don Justo llamó a Modesto. Modesto, a su vez, llamó a un contacto que había hecho a través del canal reformado: un ingeniero de ciberseguridad llamado Bruno Castejón que colaboraba ocasionalmente con una de las fundaciones que ahora patrocinaban el canal y que tenía experiencia específica en lo que el sector llama *ciberseguridad automotriz*.

La videollamada a tres bandas —don Justo desde su despacho, Modesto desde su estudio improvisado, Bruno desde algún lugar que tenía detrás una pizarra llena de diagramas— empezó con Bruno haciendo la pregunta que iba a estructurar todo lo que vino después:

—Antes de nada: ¿el coche ha estado en algún taller no oficial recientemente?
¿Algo que no sea el concesionario de la marca?

Don Justo no lo sabía. Pero Felisa, consultada esa misma tarde, sí lo recordaba: dos meses antes del primer incidente, había llevado el coche a un taller multimarca de Tomelloso para una revisión rutinaria y el cambio de una pieza del

sistema de frenado que, según el taller, *"no era necesario hacerlo en el oficial, salía más barato y quedaba igual"*.

Bruno asintió, en la pantalla, con la expresión de quien ve confirmarse una hipótesis que no quería tener que confirmar.



De lo que Bruno explicó sobre los coches modernos

—Voy a explicar esto de la manera más sencilla que pueda, porque es importante que se entienda bien, y luego entro en lo técnico para quien quiera. Un coche moderno, de los últimos diez años, no es una máquina mecánica con algo de electrónica encima. Es, literalmente, una red de ordenadores sobre ruedas. Decenas de unidades de control electrónico —lo que en el sector llamamos ECUs— que gestionan el motor, los frenos, la dirección asistida, el airbag, el aire acondicionado, el infoentretenimiento... todo. Y todas esas unidades se comunican entre sí a través de una red interna, generalmente un protocolo llamado **CAN bus**, que en muchos modelos no tiene apenas seguridad: si alguien consigue acceso a esa red, puede enviar mensajes que las ECUs obedecen sin preguntar mucho.

—El acceso a esa red se hace normalmente a través de un puerto físico llamado **OBD-II**, que está debajo del salpicadero en casi todos los coches y que existe precisamente para que los talleres puedan diagnosticar el vehículo. Cualquier mecánico conecta ahí un dispositivo de diagnóstico, lee los códigos de error, hace su trabajo.

—El problema empieza cuando ese puerto, o el software que se actualiza a través de él, queda en un estado que no debería. Hay dispositivos de diagnóstico de talleres no oficiales que, para abaratar costes o por desconocimiento, usan software desactualizado o mal configurado. Y algunos de esos dispositivos, sin que el taller lo sepa ni lo pretenda, dejan tras de sí

configuraciones de red más permisivas de lo que deberían: certificados caducados, módulos de comunicación que quedan en modo de depuración, o directamente puertas de acceso remoto que el fabricante había cerrado y que el proceso de diagnóstico, mal ejecutado, vuelve a abrir.

Don Justo escuchaba con la libreta azul —rehabilitada para la ocasión, esta vez con un propósito legítimo— tomando notas.

—¿Y eso significa que alguien, desde fuera, puede mover el volante? —preguntó.

—En según qué modelos y configuraciones, sí. No es ciencia ficción: en 2015, dos investigadores de seguridad demostraron públicamente que podían tomar el control remoto de un vehículo conectado, incluyendo la dirección y los frenos, explotando vulnerabilidades de este tipo. Desde entonces los fabricantes han mejorado mucho, hay normativas específicas, pero la cadena de seguridad es tan fuerte como su eslabón más débil. Y el eslabón más débil, casi siempre, es el punto donde un humano con prisa conecta un dispositivo barato a un puerto que da acceso a todo.

— ★ —

Del diagnóstico y de lo que encontraron

Con el consentimiento de Felisa, Bruno —desplazándose un sábado hasta Tomelloso, en lo que él mismo llamó *"trabajo de campo poco habitual para alguien que normalmente analiza cosas desde un ordenador"*— conectó al puerto OBD-II del coche un equipo de diagnóstico propio, certificado, y revisó la configuración de las unidades de control relacionadas con la dirección asistida y la conectividad.

Lo que encontró confirmó, con una precisión que a Felisa le produjo una mezcla de alivio y escalofrío, todo lo que ella había estado diciendo durante dos meses.

El módulo de comunicaciones del vehículo —el que gestiona la conexión con la aplicación móvil y las actualizaciones del fabricante— tenía un certificado de seguridad caducado desde la revisión en el taller no oficial. Ese certificado caducado no impedía que el coche funcionara con normalidad para su propietaria, pero sí dejaba el canal de comunicación en un estado donde, en teoría, una conexión externa que conociera esa vulnerabilidad específica podía establecer comunicación con las unidades de control sin la autenticación que el fabricante exigía normalmente.

En román paladino, como diría don Justo más tarde en la asociación: el taller, sin ninguna mala intención, había dejado una ventana abierta en un piso que de otro modo habría estado cerrado a cal y canto. Y por esa ventana, en dos ocasiones, había entrado algo o alguien.

Lo que no pudieron determinar con certeza —y Bruno fue muy claro en que esto era una limitación real, no una evasiva— fue *quién* había entrado. Las hipótesis iban desde un ataque dirigido específicamente contra Felisa, lo cual parecía improbable porque no había ningún motivo aparente, hasta —la hipótesis que Bruno consideraba más plausible— un escaneo automatizado y no dirigido: programas que rastrean internet buscando vehículos con esa vulnerabilidad concreta, sin objetivo específico, y que al encontrar uno, prueban comandos básicos solo para verificar que la vulnerabilidad es real. Una especie de "*está abierto, vamos a ver qué pasa si empujamos la puerta*", sin que quien empuja la puerta tenga ningún plan más allá de comprobar que se abre.

Esto, dijo Bruno, no hacía el caso menos grave. Lo hacía, en cierto modo, más grave: significaba que no había sido un ataque excepcional contra una persona concreta, sino la manifestación visible de un problema que podía estar afectando, en silencio, a una cantidad desconocida de vehículos con la misma vulnerabilidad, cuyos propietarios no tenían ningún motivo para sospechar nada porque, a

diferencia de Felisa, quizá nunca habían notado el momento exacto en que alguien empujó la puerta.



De la normativa que existía y de por qué no había bastado

Inés, a quien don Justo llamó esa misma noche con el informe de Bruno delante, conocía la normativa relevante: el reglamento internacional conocido como **UNECE R155**, que desde 2022 exige a los fabricantes de vehículos disponer de un Sistema de Gestión de Ciberseguridad certificado, capaz de identificar y mitigar amenazas durante todo el ciclo de vida del vehículo, incluyendo las actualizaciones remotas.

—La normativa existe y es exigente —dijo Inés— y obliga al fabricante. El problema de este caso no es que el fabricante no cumpliera la normativa. El problema es que la cadena de seguridad no termina en el fabricante. Termina en el último eslabón que toca el vehículo, que en este caso fue un taller multimarca haciendo un cambio de pieza barato y legítimo, usando una herramienta de diagnóstico que probablemente ni ellos sabían que tenía un problema de configuración.

—Esto es exactamente el mismo patrón que hemos visto en otros capítulos, solo que con ruedas. El phishing de Aurelio no era un fallo del banco: era un fallo en el último metro de la cadena, el clic. Aquí no es un fallo del fabricante: es un fallo en el último metro de la cadena, el puerto de diagnóstico. La seguridad de un sistema complejo no se mide por su parte más fuerte. Se mide por su parte más débil, y la parte más débil casi siempre es donde un proceso humano, hecho con prisa o sin formación suficiente, interactúa con el sistema.



De lo que pasó después, que fue menos espectacular de lo que cualquier canal de true crime habría querido

No hubo una persecución. No hubo una revelación dramática sobre quién había manipulado el coche de Felisa, porque, con toda probabilidad, nadie había manipulado el coche de Felisa específicamente: alguien, en algún lugar, había encontrado una puerta abierta y la había empujado, sin saber ni importarle de quién era la casa.

Lo que sí hubo fue lo siguiente: Bruno documentó el caso, con el consentimiento de Felisa y sin datos que la identificaran, y lo remitió al fabricante del vehículo y a la herramienta de diagnóstico del taller no oficial, que resultó ser un software de uso muy extendido entre talleres multimarca de toda España. El fabricante de la herramienta confirmó la vulnerabilidad, ya conocida en círculos especializados, pero no resuelta en las versiones que muchos talleres seguían usando, y publicó una actualización urgente.

El concesionario oficial, esta vez con la información de Bruno en la mano, revisó el coche de Felisa, actualizó el certificado caducado y cerró la vulnerabilidad. Felisa no volvió a notar nada extraño en el volante.

Modesto hizo un episodio. Con las cinco condiciones de Inés, sin nombrar a Felisa, sin recreaciones del momento del volante girando solo, centrado en el mecanismo: qué es el puerto OBD-II, qué deben preguntar los conductores a sus talleres, por qué una revisión más barata en un taller no oficial puede tener costes que no aparecen en la factura. El episodio se tituló *"Tu coche es un ordenador con ruedas: lo que deberías saber antes de tu próxima revisión"*, sin signos de exclamación, sin miniatura en rojo.

Tuvo seis mil visualizaciones. Menos que cualquier episodio de la época antigua del canal. Pero entre los comentarios había uno de un mecánico de un taller de

Albacete que decía que iba a revisar esa misma semana el software de sus equipos de diagnóstico, "*por si acaso*".



Don Justo, esa noche, escribió en la libreta azul —que ya no era de cosas *puntuales*, sino que se había convertido, sin que nadie lo decidiera formalmente, en el cuaderno de los casos de la asociación— una sola entrada:

Felisa Roldán. Caso resuelto. Nadie tenía la culpa de manera individual y todo el mundo tenía un poco de responsabilidad: el taller, el software, el fabricante, la prisa. Como casi siempre. La diferencia es que esta vez lo investigamos entre tres, y entre tres se ve mejor.

Cerró la libreta. Llamó a Cancerbero, que a sus catorce años ya no caminaba tanto como antes y salieron a dar el paseo corto, el de después de cenar, el que ahora hacían en lugar del largo.

Pasaron por delante del taller de coches de la plaza, que llevaba un cartel nuevo en el escaparate anunciando revisiones. Don Justo lo miró un momento. No anotó nada. Pero al día siguiente, cuando Remedios le preguntó si todo iba bien con el coche, él dijo que sí, que todo bien, y que la próxima revisión la harían en el oficial, "*por si acaso*", y Remedios, que llevaba más de un año observando los cambios pequeños en su marido con la atención de quien ha aprendido a valorarlos, no dijo nada más. Pero sonrió.

La ciberseguridad de los vehículos conectados es un campo regulado a nivel internacional mediante el reglamento UNECE R155, que exige a los fabricantes Sistemas de Gestión de Ciberseguridad certificados. Sin embargo, la cadena de seguridad incluye también a talleres, herramientas de diagnóstico y mantenimiento. Recomendaciones prácticas: utilizar talleres que mantengan actualizado su software de diagnóstico, preguntar si las actualizaciones del vehículo están al día y prestar atención a comportamientos anómalos del vehículo (movimientos del volante, frenado o aceleración no iniciados por el conductor), comunicándolos al fabricante y si se sospecha un incidente de ciberseguridad, también a las autoridades de tráfico.

No son casos. Son personas.

Esta obra es el resultado del trabajo creativo de sus autores. Para determinadas tareas de apoyo —como la organización de información, la estructuración de materiales y la asistencia en procesos de edición— se han empleado herramientas de inteligencia artificial. No obstante, la concepción, autoría, criterio y responsabilidad sobre los contenidos pertenecen exclusivamente a los autores humanos.