

DULCINEA DEL TRUE CRIME II — EXPEDIENTE LLAVE

De cómo un número de teléfono era mucho más que un número de teléfono y de lo que ocurrió cuando alguien lo entendió antes que su dueña

Nuevos casos, mismas personas

Pilar Santamaría tenía cincuenta y ocho años, trabajaba como administrativa en una empresa de logística de Valverde de la Siega y llevaba el mismo número de teléfono desde hacía diecisiete años, que era el tiempo que le había parecido suficiente para no cambiar algo que funcionaba. El número estaba en la tarjeta de su médico de cabecera. En la app del banco. En el perfil de su correo electrónico como número de recuperación. En el portal de la Seguridad Social. En el de Hacienda. En el de su mutua. En el de la empresa donde trabajaba para recibir las nóminas. En la agenda de todos los que la conocían.

Era, en todos los sentidos relevantes, mucho más que un número de teléfono. Era la llave de su identidad digital completa. Y Pilar no lo sabía porque nadie se lo había explicado. Porque nadie explica estas cosas hasta que algo sale mal.

Algo salió mal un miércoles de septiembre.

— ★ —

De lo que ocurrió antes de que Pilar lo supiera

Lo que ocurrió antes de que Pilar lo supiera duró probablemente varias semanas y ocurrió en varios pasos que solo son visibles en retrospectiva, cuando alguien los reconstruye con la paciencia de quien tiene todos los fragmentos y el tiempo de ordenarlos.

Alguien había obtenido los datos de Pilar. No todos de golpe: los datos se obtienen por capas, como una cebolla que se pela despacio. El nombre y los apellidos son públicos en muchos contextos. El número de teléfono también. La fecha de nacimiento suele estar en redes sociales. La dirección puede obtenerse de registros públicos o de bases de datos filtradas que circulan en foros específicos. Lo que faltaba, para completar el perfil con la precisión que algunos procedimientos requieren, era el documento de identidad.

El documento de identidad llegó de la manera más sencilla posible: alguien se lo pidió a Pilar con una excusa que en el momento sonó razonable. No hace falta saber cuál fue la excusa porque las excusas varían y lo que importa no es la excusa sino el mecanismo: alguien construyó una situación en la que Pilar sintió que enviar una fotografía de su DNI por WhatsApp era lo que cualquier persona haría en esa circunstancia. Y lo envió.

Después de eso, Pilar no notó nada durante un tiempo. Eso también es parte del mecanismo: el período de silencio entre la entrega de la información y el primer síntoma del daño, que puede durar días o semanas y que hace más difícil la reconstrucción posterior porque la víctima no sabe cuándo empezó exactamente.

Lo que ocurrió durante ese silencio, reconstruido después con la información de la operadora y la denuncia policial, fue lo siguiente: alguien se presentó ante la operadora de Pilar, o lo hizo de manera telemática, con datos suficientes para que el sistema de verificación los considerara válidos. Solicitó una portabilidad del número a otra operadora. La portabilidad se ejecutó. Y el número de teléfono que Pilar llevaba diecisiete años usando y que era la llave de su identidad digital completa pasó a estar bajo el control de alguien que ella no conocía.



PRIMERA PARTE

Los cuatro golpes o de cómo el daño llegó en oleadas

El primer golpe: el teléfono que deja de funcionar

El miércoles a media mañana, Pilar miró el móvil para responder un mensaje y vio que no había cobertura. Comprobó si era el edificio. Salió a la calle. Siguió sin cobertura. Reinició el teléfono. Nada. Llamó a la operadora desde el fijo de la oficina y esperó veintidós minutos en la cola de atención al cliente.

La operadora le informó de que su número había sido portado a otra compañía a petición del titular. Pilar explicó que ella era la titular y que no había solicitado ninguna portabilidad. La operadora le dijo que abriría una incidencia y que en un plazo de cuarenta y ocho horas recibiría respuesta. Cuarenta y ocho horas es mucho tiempo cuando el teléfono es la llave de todo lo demás.

En esas primeras horas, Pilar no entendía todavía la dimensión de lo que estaba pasando. Pensaba en un error burocrático, en un cruce de expedientes, en una de esas cosas absurdas que ocurren a veces con las operadoras y que se resuelven con una llamada y una disculpa. No pensaba en lo que tenía en el número de teléfono. No pensaba en las llaves.



El segundo golpe: la llamada del supuesto nuevo titular

Esa misma tarde, desde un número desconocido, recibió una llamada en el teléfono fijo de su casa. Era un hombre que se identificó con un nombre que ella no reconoció y que le dijo, con una naturalidad que le resultó más perturbadora que cualquier amenaza, que había comprado un teléfono con esa línea en una

tienda de Barcelona y que quería saber si había algún problema con el número porque no podía hacer llamadas.

Pilar tardó un momento en entender lo que estaba escuchando. El hombre no sonaba nervioso. No sonaba amenazante. Sonaba como alguien que había comprado algo y tenía un problema técnico. Lo cual podía significar dos cosas: que era una víctima secundaria que había adquirido un terminal con una línea fraudulenta sin saberlo o que era parte del esquema y estaba llamando para evaluar hasta dónde llegaba el control que tenía sobre la situación.

Pilar colgó. Le temblaban las manos. Y entonces, por primera vez desde que el teléfono había dejado de funcionar, empezó a pensar en las llaves.

*El banco. El correo. La Seguridad Social. Hacienda. La mutua.
WhatsApp. Todo vinculado al mismo número. Todo accesible para
quien controle ese número.*

— ★ —

El tercer golpe: la llamada extorsiva

La llamada extorsiva llegó al día siguiente, también al fijo. Una voz que no ponía nombre, que no explicaba cómo había obtenido el número del fijo y que le dijo a Pilar que tenía acceso a información suya que ella no querría que circulara y que si quería que eso no ocurriera había cosas que podía hacer.

No especificó qué información. No especificó qué cosas. La amenaza vaga es en muchos casos más eficaz que la específica porque activa en la víctima todos los miedos simultáneamente: el miedo a lo que el atacante sabe, el miedo a lo que puede hacer con ello, el miedo a lo que uno no sabe que el atacante sabe.

Pilar colgó. Llamó a su hija. Su hija le dijo que llamara a la policía. Pilar llamó a la policía.



El cuarto golpe: el laberinto

El cuarto golpe no fue una llamada. Fue lo que vino después: el proceso de reclamar, denunciar y recuperar lo que había sido sustraído, que resultó ser un laberinto con tantas puertas como organismos y con ninguna puerta que llevara directamente al centro.

La operadora abrió una incidencia. La incidencia tardó más de cuarenta y ocho horas. Mientras tanto, Pilar no tenía acceso a su banco por la app porque el segundo factor de autenticación llegaba por SMS al número que ya no era suyo. No podía recuperar su correo electrónico porque el número de recuperación era el mismo. No podía gestionar ningún trámite con la Seguridad Social ni con Hacienda a través de los portales que requerían verificación por SMS.

Era como si le hubieran cambiado la cerradura de todas las puertas al mismo tiempo y las llaves nuevas estuvieran en manos de otro.

En comisaría tomaron la denuncia con eficiencia y con la honestidad de quien sabe que el proceso va a ser largo: le explicaron que el caso pasaría a la unidad de delitos informáticos, que requerirían información a la operadora, que los plazos de la investigación dependían de muchos factores y que era difícil dar una estimación. Le dieron un número de atestado. Le desearon suerte.

En la CNMC, el organismo regulador de las telecomunicaciones, presentó una reclamación por portabilidad no consentida. Le informaron del procedimiento, de los plazos, de la documentación necesaria. Todo correcto, todo por escrito, todo lento.

En la AEPD presentó otra reclamación, esta vez por el tratamiento indebido de sus datos personales: alguien había usado su DNI para suplantar su identidad ante una operadora de telecomunicaciones. La AEPD tenía competencia para investigar si la operadora había cumplido con sus obligaciones de verificación de identidad antes de ejecutar la portabilidad. También tenía plazos. También tenía procedimientos.

Pilar tenía tres expedientes abiertos en tres organismos distintos, ninguno coordinado con los otros, y seguía sin teléfono.



SEGUNDA PARTE

Lo que don Justo aprendió y lo que Inés y Modesto explicaron

Don Justo supo del caso de Pilar a través de Darío, el portero, cuya madre conocía a Pilar de la cooperativa. No fue una consulta formal: fue una conversación en el portal, un *a ver si sabes qué se puede hacer*, que era la forma en que muchas de las conversaciones más importantes de los últimos años habían empezado.

Don Justo escuchó el relato, anotó lo esencial en la libreta azul y luego hizo lo que había aprendido a hacer: antes de decir nada, llamó a quien sabía más que él.



De lo que Modesto y Bruno explicaron sobre el mecanismo

Modesto había preparado con Bruno Castejón, el ingeniero de ciberseguridad, un episodio sobre SIM swapping y portabilidad fraudulenta que llevaba semanas en el borrador esperando un caso concreto que lo anclara a la realidad. El caso de Pilar, sin su nombre, era exactamente lo que necesitaba.

—Hay que distinguir dos mecanismos que a veces se confunden porque producen el mismo resultado desde el punto de vista de la víctima: se queda sin teléfono y otra persona tiene el control de su número. Pero el procedimiento es diferente y eso importa para entender las responsabilidades.

—El **SIM swapping** es la solicitud de un duplicado de la SIM a la propia operadora: el atacante se hace pasar por el titular, alega que ha perdido el teléfono o que necesita un duplicado, y consigue que la operadora emita una nueva SIM con el mismo número. En el momento en que la nueva SIM se activa, la SIM original deja de funcionar. El atacante recibe todos los SMS dirigidos al número, incluidos los códigos de autenticación de bancos, correos, plataformas. La víctima nota que el teléfono ha dejado de funcionar, pero en esos primeros minutos o horas de confusión el atacante ya puede haber accedido a todo.

—La **portabilidad fraudulenta** es diferente: el atacante no solicita un duplicado a la misma operadora, sino que tramita una portabilidad a otra operadora diferente, haciéndose pasar por el titular. El número pasa a estar bajo la operadora del atacante, que emite una SIM nueva. El resultado es el mismo: la víctima pierde el control del número. Pero la trazabilidad es diferente porque involucra a dos operadoras y a la CNMC como regulador de las portabilidades.

—En ambos casos el dato que hace posible la suplantación es la combinación de información personal verificable: nombre, apellidos, DNI, fecha de

nacimiento, en algunos casos dirección o últimas cifras de la cuenta bancaria vinculada. Cuanta más información tiene el atacante, más fácil le resulta superar los controles de verificación de la operadora. Y cuanto más deficiente es el protocolo de verificación de la operadora, menos información necesita.

Bruno añadió algo que don Justo anotó con atención:

—La AEPD sancionó a Vodafone en agosto de 2026 con más de un millón de euros por, entre otras cosas, haber activado una línea no autorizada y haber entregado datos personales a un tercero por una verificación de identidad deficiente. Eso nos dice dos cosas: que el problema de los protocolos de verificación de las operadoras es real y documentado, y que las instituciones tienen competencia para investigarlo y sancionarlo cuando ocurre. Lo que no nos dice es que la víctima vaya a ver resuelta su situación en un plazo razonable.

— ★ —

De lo que Inés explicó sobre la revictimización institucional

Inés escuchó el relato del laberinto de Pilar con la atención concentrada de quien reconoce un patrón que ha estudiado y que sigue produciendo indignación, aunque ya no sorprenda.

—Lo que describe el caso de Pilar en su fase posterior al descubrimiento del fraude es lo que en victimología se llama **revictimización institucional**: el proceso por el cual los sistemas diseñados para proteger a las víctimas acaban generando daño adicional sobre ellas, no por mala intención sino por la suma de procedimientos que no están coordinados, plazos que no tienen en cuenta la urgencia del caso desde el punto de vista de la víctima, y la carga de prueba y documentación que recae sobre quien ya ha sufrido el daño.

—Pilar tenía tres expedientes abiertos en tres organismos distintos. Ninguno de esos organismos tenía obligación de coordinarse con los otros ni de informar a Pilar de en qué punto estaban los otros dos. La investigación penal en la policía no se comunica automáticamente con el procedimiento administrativo en la CNMC ni con la reclamación en la AEPD. Pilar tenía que mantener los tres procesos simultáneamente, cada uno con su documentación, sus plazos, sus formularios y sus silencios institucionales.

—Y mientras tanto seguía sin teléfono. O con un teléfono nuevo con un número nuevo que no era el suyo, que no estaba en la tarjeta de su médico ni en el portal de su banco ni en la agenda de nadie que la conociera. Un número nuevo es, para alguien de cincuenta y ocho años con diecisiete años con el mismo número, casi una identidad nueva. Y nadie le preguntó si quería una identidad nueva.

—La revictimización institucional no siempre viene de la incomprensión. A veces viene del exceso de comprensión burocrática: cada organismo entiende perfectamente su parte del problema y no tiene capacidad ni mandato para ver el conjunto. El resultado es que la víctima, que es la única que ve el conjunto porque lo está viviendo, tiene que hacer el trabajo de coordinación que el sistema no hace. Y eso, cuando uno acaba de perder el control de toda su identidad digital, es una carga que no debería existir.

Don Justo escuchó todo esto y luego dijo algo que Inés no esperaba:

—¿Y qué se le dice a Pilar mientras tanto? ¿Que tenga paciencia?

—No —dijo Inés—. Se le dice que lo que le ha pasado tiene nombre, que hay organismos que tienen competencia para investigarlo, que el proceso va a ser más largo de lo razonable y que eso no es culpa suya. Y se le acompaña mientras dura, que es lo que el sistema no hace y que es lo único que no puede sustituirse con un procedimiento.



TERCERA PARTE

Del número de teléfono como llave o de la dependencia que nadie explicó

Fue durante la conversación con Inés cuando don Justo planteó la reflexión que llevaba días rondándole y que no había sabido formular con precisión hasta ese momento:

—Lo que me parece más grave de todo esto no es el fraude en sí. Es que Pilar no sabía que su número de teléfono era la llave de todo lo demás. Nadie se lo había dicho. Y si ella no lo sabía, es razonable pensar que la mayoría de las personas que tienen un teléfono tampoco lo saben.

Inés asintió.

—Tiene razón. Y eso es el problema más profundo del caso: no el modus operandi del atacante, que es sofisticado pero documentado y prevenible, sino el hecho de que hemos construido una infraestructura de identidad digital que depende de manera crítica del número de teléfono sin haber explicado a los ciudadanos que eso es así. El número de teléfono empezó siendo un medio de comunicación. Se convirtió, de manera gradual e invisible, en el segundo factor de autenticación universal de toda la vida digital de una persona.

—El banco lo usa para confirmar transferencias. El correo lo usa como número de recuperación cuando olvidas la contraseña. La Seguridad Social lo usa para verificar identidad en los trámites online. Hacienda lo usa para los códigos de

acceso. La mutua para las citas. WhatsApp está vinculado al número de manera indisoluble: si pierdes el número, pierdes el acceso a todos tus mensajes y contactos. Y los contactos, que es algo en lo que casi nadie piensa, son en sí mismos un activo de enorme valor: contienen la agenda de toda tu vida social, laboral y familiar, con nombres, números y en muchos casos fotografías.

Don Justo pensó en su propio teléfono. En todo lo que había en él y que él no había pensado que estaba en él.

El médico. El banco. El seguro. El correo. Las fotos de Sofía. Los mensajes de Remedios. Los contactos de la asociación. Todo en un número que elegí hace doce años porque era fácil de recordar.

— ★ —

De Modesto, que lo explicó mejor que nadie en cuatro minutos

El episodio de Modesto sobre SIM swapping duró diecinueve minutos y tuvo doce mil visualizaciones en la primera semana, que era el mejor resultado del canal desde el episodio sobre el cargador del vehículo eléctrico. Pero lo que don Justo recordó de ese episodio no fue ningún dato técnico sino los cuatro minutos finales, donde Modesto hablaba sin Bruno, solo, con la cadencia de quien ha pensado mucho en algo y lo dice con las palabras justas:

—Llevamos unos quince años construyendo nuestra vida digital sobre el teléfono móvil. Lo hemos llenado de aplicaciones, de cuentas, de contraseñas, de contactos, de fotos, de documentos, de conversaciones. Lo hemos convertido en el archivo central de nuestra vida. Y al mismo tiempo hemos dejado que el número de teléfono, que es la dirección de ese archivo, sea verificable con los mismos datos que cualquiera puede obtener con un poco de tiempo y las herramientas adecuadas.

—No es culpa de quien lo pierde. Es una vulnerabilidad del sistema que el sistema no ha resuelto y que no ha explicado. Las operadoras no te avisan cuando contratas de que tu número es la llave de tu banco. Los bancos no te avisan de que si pierdes el número pierdes el segundo factor de autenticación. La Administración no te avisa de que sin ese número no puedes gestionar tus propios trámites online. Nadie te avisa de nada. Y cuando pasa, te encuentras solo frente a un laberinto de procedimientos mientras alguien que tiene tu número decide qué hacer con la llave de tu vida digital.

—Lo que se puede hacer, que no es suficiente, pero es lo que hay: revisar qué cuentas tienen vinculado tu número de teléfono como factor de recuperación y dónde es posible sustituirlo por una aplicación de autenticación que no depende del número. Activar alertas en tu banco para cualquier operación. Y si alguna vez el teléfono deja de funcionar sin explicación aparente, llamar inmediatamente a la operadora desde otro dispositivo, no esperar.

Don Justo vio el episodio entero dos veces. Luego llamó a Macarena y le preguntó qué aplicaciones tenía vinculadas a su número de teléfono como factor de recuperación.

—Todas —dijo Macarena, después de un silencio.

—Todas cuáles.

—Todas las que uso. El banco, el correo, las redes. ¿Por qué?

—Te mando un enlace —dijo don Justo—. Míralo cuando puedas. Y luego hablamos.

— ★ —

De lo que pasó con Pilar, con sus plazos reales

La operadora tardó cuatro días en recuperar el número para Pilar, que fue el plazo que la CNMC establece como máximo para la reversión de una portabilidad

fraudulenta cuando se acredita que no fue consentida. Cuatro días es un plazo que en el papel parece razonable y que en la práctica significa cuatro días sin acceso al banco, al correo, a la Seguridad Social, a WhatsApp y a cualquier servicio que use ese número como factor de verificación.

La investigación policial siguió su curso con los plazos de la investigación penal, que son más largos. El expediente de la AEPD sobre la posible deficiencia en la verificación de identidad de la operadora también siguió su curso. Pilar recibió cartas. Pilar respondió cartas. Pilar aportó documentación. Pilar esperó.

Lo que nunca recuperó o que tardó mucho más en recuperar, fue la sensación de que su teléfono era simplemente un teléfono. De que el número era un número. De que la llave estaba en su bolsillo y no podía ser copiada mientras ella no la prestara.

Don Justo lo anotó en la libreta azul, en la página que había reservado para el caso de Pilar, con la letra pequeña de los apuntes importantes:

El daño técnico se repara. El daño en la sensación de control sobre la propia vida digital es más lento de reparar. Nadie lo mide en los procedimientos. Nadie lo compensa en las resoluciones. Pero está ahí.

Cancerbero dormía bajo la mesa. Remedios leía en el salón. Don Justo cogió su teléfono, entró en la configuración y buscó, por primera vez en doce años de tener ese número, la sección de seguridad de su cuenta de correo para ver qué tenía vinculado. El número de teléfono aparecía como único método de recuperación.

Lo cambió esa noche. Era tarde, y Remedios le preguntó qué hacía.

—Cambiar la cerradura —dijo don Justo.

—¿De qué?

—De casi todo.

Remedios lo miró con la expresión de quien lleva años acostumbrándose a las respuestas de don Justo y que ha aprendido que cuando no las entiende del todo es mejor esperar a que él las explique, que tarde o temprano lo hace.

Don Justo la explicó esa noche, en la cocina, mientras se enfriaba el último café. Y Remedios, cuando entendió, sacó su propio teléfono y le preguntó si le podía ayudar a hacer lo mismo.

El SIM swapping y la portabilidad fraudulenta son delitos tipificados en el Código Penal español bajo los artículos relativos a la usurpación de identidad, el acceso no autorizado a sistemas informáticos y el fraude. Si su teléfono deja de funcionar sin explicación: llame inmediatamente a su operadora desde otro dispositivo; si confirman un cambio no solicitado, exija la reversión inmediata indicando que es una portabilidad o cambio de SIM fraudulento; presente denuncia en comisaría o Guardia Civil; presente reclamación ante la CNMC (cnmc.es) por portabilidad no consentida; presente reclamación ante la AEPD (aepd.es) si sus datos personales fueron utilizados sin consentimiento; contacte con su banco inmediatamente para bloquear operaciones que requieran verificación por SMS. Para reducir el riesgo: active una aplicación de autenticación (Google Authenticator, Microsoft Authenticator u otras) como segundo factor en lugar del SMS siempre que la plataforma lo permita; revise qué cuentas tienen su número como único método de recuperación; active alertas de operaciones en su banco. El número de teléfono es hoy la llave de su identidad digital. Trátelo como tal.

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.