DULCINEA DEL TRUE CRIME III — EXPEDIENTE X

De cómo alguien que parecía Alejandro Fierabrás no era Alejandro Fierabrás y de por qué Amparo Ruiz llamó al móvil antes de transferir

Lo que don Justo escuchó en una sola llamada, porque esta vez no hizo falta más

---

Hay casos que se resuelven antes de convertirse en casos. Este es uno de esos. Lo cuento de todas formas porque lo que casi ocurre importa tanto como lo que ocurre y porque la diferencia entre los dos la hizo una llamada de teléfono que duró menos de un minuto.

Me lo contó Inés un miércoles por la tarde, con la voz de quien acaba de recibir una noticia que es a la vez buena y preocupante y que no sabe muy bien por cuál de las dos empezar. Empezó por la buena, que era lo que había pasado. Luego llegó la preocupante, que era lo que había estado a punto de pasar.

Cancerbero estaba en su sitio. La libreta azul estaba abierta. Todo en orden para recibir lo que venía.

— ✶ —

De Amparo Ruiz, que llevaba veinte años haciendo bien su trabajo sin que nadie lo notara

Amparo Ruiz era la directora financiera de Fierabrás e Hijos desde hacía veinte años. En los cinco episodios de los WARNING no había aparecido porque hacía bien su trabajo sin que hubiera ninguna razón para aparecer, que es exactamente la situación más frecuente y menos reconocida en cualquier empresa.

Conocía a Alejandro desde que Alejandro tenía treinta y dos años y acababa de heredar la empresa de su padre con la mezcla de orgullo y pánico que produce heredar algo que quieres

pero que todavía no sabes si sabes llevar. Había visto pasar los buenos años y los menos buenos. Había gestionado los números del caso Marcos con la discreción que el caso requería. Y había leído el informe de Inés, la sección de cumplimiento normativo, con la atención de quien sabe que lo que está leyendo no es burocracia sino sentido común puesto por escrito.

La recomendación que había subrayado, con un bolígrafo azul en el margen, era esta:

> *Ante cualquier solicitud de transferencia urgente o confidencial que llegue por un canal no habitual, verificar siempre por un segundo canal independiente antes de ejecutar. La urgencia y la confidencialidad son los dos elementos más frecuentes en los intentos de fraude corporativo. Su combinación debe activar siempre el protocolo de verificación, independientemente de quién parezca ser el solicitante.*

Amparo había subrayado eso en octubre. En febrero, ese subrayado le ahorró a Fierabrás e Hijos ochenta mil euros.

— ✶ —

De la videollamada, que parecía Alejandro, pero no lo era

Era un martes por la mañana. Alejandro estaba de camino a una reunión con un cliente en otra ciudad y Amparo sabía que estaba viajando porque lo sabía siempre, porque llevar las finanzas de una empresa implica saber dónde está quien toma las decisiones.

La videollamada llegó desde el número de móvil de Alejandro, que Amparo tenía guardado, a las diez y cuarto. La imagen era Alejandro: la cara, la voz, el gesto de pasarse la mano por el pelo cuando estaba explicando algo que le parecía importante. El fondo era el interior de un coche, que era coherente con que estuviera viajando.

Lo que Alejandro le dijo, con la naturalidad de quien está resolviendo un asunto mientras conduce, era esto: habían cerrado un acuerdo con un proveedor estratégico de logística

refrigerada que llevaban meses negociando. El contrato todavía no era público porque el proveedor tenía compromisos con competidores que no podían saber que habían perdido la negociación. Necesitaba que Amparo hiciera una transferencia de ochenta mil euros como señal, a una cuenta que le iba a mandar por mensaje, antes del mediodía. Urgente y confidencial. Ya hablarían del resto cuando llegara.

Amparo escuchó todo esto mirando la cara de Alejandro en la pantalla del ordenador.

Luego cogió el teléfono fijo de su mesa y llamó al móvil personal de Alejandro. El segundo canal. El que Inés había recomendado en el informe.

Alejandro contestó al segundo tono desde la autopista, con el manos libres del coche, sin saber nada de ninguna videollamada y sin haber enviado ningún mensaje con ningún número de cuenta.

—¿Amparo? ¿Pasa algo?

—Puede que sí —dijo Amparo—. Ahora mismo alguien que parece usted me está pidiendo por videollamada que transfiera ochenta mil euros antes del mediodía.

Hubo una pausa.

—Yo estoy en la autopista desde las ocho —dijo Alejandro—. No he llamado a nadie.

—Ya me lo imaginaba —dijo Amparo—. No transfiero nada.

—No transfieras nada.

—No transfiero nada —repitió Amparo, con el tono de quien confirma una decisión que ya había tomado antes de hacer la llamada.

— ✶ —

De lo que Bruno encontró en los metadatos, explicado en tiempo récord

Bruno Castejón analizó los metadatos de la videollamada esa misma tarde, después de que Alejandro lo contactara a través de Inés con la urgencia específica de quien acaba de descubrir que alguien ha usado su cara para intentar robarle.

Me lo explicó en siete minutos, que para Bruno era una velocidad que sugería que o el caso era sencillo o había decidido que yo ya tenía suficiente base para no necesitar los diecisiete minutos completos. Creo que era lo segundo y me pareció un progreso.

—El número desde el que llegó la llamada era el de Alejandro pero la llamada no salió del dispositivo de Alejandro —dijo Bruno—. Salió de un sistema de suplantación de caller ID: una tecnología que permite que una llamada parezca originarse desde cualquier número, incluyendo números reales de personas reales. Eso es la capa de entrada.

—¿Y la imagen? —pregunté.

—La imagen es un deepfake de vídeo en tiempo real. Hay sistemas disponibles ahora mismo que toman como base las imágenes públicas de una persona —LinkedIn, web de empresa, noticias, cualquier fotografía o vídeo accesible— y generan un avatar sintético que reproduce los rasgos faciales, la voz y los patrones de movimiento de esa persona. El operador humano que está detrás habla y el sistema sintetiza la voz y el rostro en tiempo real. Si la calidad de las imágenes de base es suficiente y la conexión es buena, el resultado puede ser convincente para alguien que conoce a la persona pero no la está viendo en condiciones de máxima atención.

—¿Y Alejandro tiene muchas imágenes públicas?

—Tiene una web de empresa con foto, un LinkedIn actualizado, tres entrevistas en medios locales de los últimos dos años y un vídeo de presentación en la web de una asociación empresarial provincial. Es suficiente para construir un avatar funcional.

Le pregunté si había manera de detectarlo en tiempo real.

—Hay señales —dijo Bruno—. La sincronización labial a veces falla en las consonantes complejas. Los movimientos oculares son menos naturales que en una persona real. La

resolución en los bordes del rostro puede ser ligeramente inferior. Pero detectar esas señales requiere saber que hay que buscarlas y la mayoría de las personas que reciben una videollamada de alguien que conocen no están buscando señales de deepfake. Están escuchando lo que les dicen.

—Entonces la defensa no es técnica.

—La defensa es el protocolo. Lo que hizo Amparo. Verificar por un canal independiente antes de actuar. Eso no requiere detectar el deepfake. Requiere no confiar en un solo canal aunque parezca fiable.

Le dije que lo anotaba. Lo anoté.

— ✶ —

De lo que Inés explicó y de Encarna del quinto

Inés, cuando me llamó esa tarde, había hablado ya con Alejandro y con Amparo y con Bruno, y tenía el caso ordenado de la manera en que Inés ordena las cosas cuando ha tenido tiempo de pensarlas: con la parte técnica en su sitio, la parte humana en su sitio y la reflexión de fondo en el lugar que le corresponde.

—Lo que ha intentado hacer con Fierabrás e Hijos se llama fraude al CEO —me dijo—, aunque el nombre es un poco engañoso porque la víctima no es el CEO sino quien recibe la instrucción aparentemente del CEO. En su versión clásica llegaba por correo electrónico con un dominio falsificado. En su versión actual llega por videollamada con un avatar generado por IA. El mecanismo psicológico es exactamente el mismo en las dos versiones: urgencia, confidencialidad y la autoridad de quien parece ser el jefe.

—¿Y por qué Fierabrás e Hijos? —pregunté.

—Probablemente porque está en el registro mercantil, tiene web pública, tiene presencia en medios locales después del proceso de los últimos meses y Alejandro tiene suficiente presencia digital para construir un avatar convincente. No es un objetivo elegido con precisión quirúrgica. Es un objetivo que cumple los criterios básicos y que alguien ha encontrado buscando empresas de tamaño medio con directivos con presencia pública.

Luego Inés dijo algo que yo ya estaba pensando:

—¿Recuerda el caso de Encarna?

Le dije que sí. Que por supuesto.

—El mecanismo es el mismo. Un perfil que parece de confianza. Una historia coherente con lo que la víctima ya sabe. Urgencia que impide la verificación. Y la tecnología que hace que lo que antes requería esfuerzo —construir una identidad falsa creíble— ahora sea accesible para cualquiera con un ordenador y las imágenes públicas adecuadas. Encarna recibió mensajes escritos de alguien que parecía Marco. Amparo recibió una videollamada de alguien que parecía Alejandro. La tecnología ha cambiado. El anzuelo es el mismo.

—¿Y la protección?

—También es la misma, en el fondo. Encarna no tenía un segundo canal porque no sabía que el primero era falso. Amparo sí lo tenía porque alguien le había dicho que lo usara. La diferencia entre las dos situaciones no es tecnológica. Es si alguien te ha explicado antes de que pase que tienes que verificar antes de actuar.

Me quedé en silencio un momento. Pensé en Encarna subiendo con Remedios al mercado los martes. En los bizcochos. En los cuatro meses de conversaciones con Marco que no existía. En la vergüenza que Encarna había tardado meses en soltar.

Le pregunté a Inés si Amparo estaba bien.

—Amparo está bien —dijo Inés—. Más que bien. Cuando Alejandro le dijo que había salvado ochenta mil euros con una llamada de un minuto, Amparo dijo que no había salvado nada, que simplemente había seguido el protocolo. Alejandro le dijo que eso era exactamente lo que había salvado los ochenta mil euros. Amparo dijo que entonces el informe había valido lo que valía.

Inés hizo la pausa que hace cuando algo le resulta satisfactorio, pero no quiere que parezca que se está felicitando a sí misma.

—¿Y usted cómo está? —le pregunté.

—Contenta —dijo—. Que es diferente de satisfecha. Satisfecha estaría si hubiera impedido el intento. Contenta estoy porque el protocolo funcionó. Que es mejor que yo.

Anoté eso también.

— ✶ —

De Alejandro, que esta vez fue la víctima y lo llevó mejor de lo que esperaba

Alejandro llegó a la empresa esa tarde después de cancelar la reunión. Llamó a Inés antes de llamar a la policía, que era el orden correcto, aunque no fuera el instintivo, porque Inés le había explicado durante los WARNING que el orden de las acciones importa cuando hay evidencia digital que puede perderse si no se preserva antes de que lleguen los técnicos.

Cuando me lo contó Inés, dijo que Alejandro había llegado al despacho con una expresión que ella describió como *la de alguien que acaba de entender algo que debería haber entendido antes y que no sabe si enfadarse o agradecérselo a quien lo ha entendido por él*.

—Lo primero que hizo fue llamar a Amparo a su despacho —me contó Inés—. Le dijo que llevaba veinte años siendo la persona más fiable de la empresa y que hoy lo había demostrado de una manera que él no iba a olvidar. Amparo dijo que solo había llamado por teléfono. Alejandro dijo que sí, que a veces lo más difícil es acordarse de hacer lo más sencillo.

Le pregunté a Inés si Alejandro había preguntado por qué lo habían elegido a él.

—Sí. Le expliqué que probablemente no lo habían elegido a él específicamente. Que buscaban empresas de tamaño medio con directivos con presencia pública suficiente para

construir un avatar. Que Fierabrás e Hijos cumplía esos criterios. Que no era nada personal.

—¿Y cómo lo llevó?

—Dijo que no sabía si eso le hacía sentir mejor o peor. Que lo pensaría.

Me pareció una respuesta honesta. La mayoría de las personas prefieren pensar que las han elegido por alguna razón a pensar que las han elegido porque salían en una búsqueda. El segundo es más probable. El primero es más cómodo.

— ✶ —

De lo que don Justo anotó y de lo que Remedios dijo sin levantar los ojos del libro

Esa noche, después de colgar, abrí la libreta azul en la página del Expediente X y escribí las dos cosas que me parecían más importantes de todo lo que había escuchado:

> *Primera: el deepfake de vídeo en tiempo real ha convertido la videollamada en un canal que ya no es verificación suficiente. Ver la cara de alguien no garantiza que sea esa persona. Eso cambia algo fundamental en cómo nos fiamos de lo que vemos.*

> *Segunda: lo que protegió a Amparo no fue saber detectar el deepfake. Fue saber que tenía que verificar antes de actuar aunque lo que veía pareciera de confianza. El protocolo como sustituto de la detección que ya no es posible.*

Luego fui al salón. Remedios leía. Le conté el caso en cuatro frases porque a estas alturas Remedios ya tiene suficiente contexto de los WARNING como para no necesitar más.

—O sea que alguien puso la cara de Alejandro en el ordenador y pidió dinero —dijo sin levantar los ojos del libro.

—Básicamente sí.

—¿Y Amparo llamó por teléfono antes de transferir?

—Exactamente.

Remedios pasó una página.

—Tendríamos que hacer eso nosotros también —dijo—. Si algún día alguien te llama por vídeo pidiéndote dinero urgente.

—Somos un portero jubilado y su mujer en Olmeda del Espino, Remedios. No creo que nadie construya un deepfake de mí para robarle a otro.

Remedios me miró por encima del libro.

—El año pasado habrías dicho lo mismo sobre las furgonetas de fontanería.

No respondí. No tenía respuesta. Y Remedios, que lo sabía, volvió a su libro con la satisfacción tranquila de quien no necesita que le den la razón porque ya la tiene.

Cancerbero me miró desde el suelo con sus ojos de galgo antiguo. Luego cerró los ojos.

Tenía razón Remedios. Como casi siempre. Y eso, que ya no me sorprende, sigue siendo suficiente para que lo anote.

El fraude al CEO o Business Email Compromise es uno de los delitos económicos de mayor crecimiento en España y Europa. En su versión más reciente utiliza deepfakes de vídeo en tiempo real que suplantan la identidad de directivos mediante avatares generados por inteligencia artificial a partir de imágenes y vídeos públicos. La protección más eficaz no es tecnológica sino procedimental: ante cualquier solicitud de transferencia urgente o confidencial, verificar siempre

por un segundo canal independiente antes de ejecutar, independientemente de quién parezca ser el solicitante y de lo convincente que resulte el canal primario. Las empresas deben incluir este protocolo en sus programas de formación en ciberseguridad y cumplimiento normativo. El caller ID spoofing, que permite que una llamada parezca originarse desde cualquier número, está tipificado como delito en España cuando se usa con fines fraudulentos. Si su empresa ha sido víctima de un intento de fraude al CEO, contacte con la Unidad de Delitos Informáticos de la Guardia Civil (GDT) o con la Brigada de Investigación Tecnológica de la Policía Nacional y preserve todas las evidencias digitales antes de formatear o modificar los dispositivos implicados. El INCIBE ofrece asesoramiento gratuito a empresas a través del teléfono 017.

No son casos. Son personas.