ARMAS DIGITALES CONTRA EL FRAUDE

Los expertos explican cómo el 'big data' y el 'machine learning' pueden utilizarse para combatir delitos financieros: hacen falta más medios e incentivos legales

POR **THIAGO FERRER**

Toda economía tiene su lado oscuro. En los primeros registros escritos, milenios atrás, los babilonios dejaron constancia de sus medidas contra el fraude en el comercio. Desde entonces, la ley y los que la cumplen han estado en perpetua carrera contra aquellos que la vulneran. Hoy, el océano de información en el que nadamos todos es amigo y enemigo en esa batalla. Por un lado, las tecnologías de la información permiten hacer planetarias estafas que antes eran exclusivas de los trileros callejeros. Pero por el otro, al igual que en el agua física, en este mar de datos la contaminación deja un rastro que puede ser localizado. Y las herramientas de *big data* y *machine learning* permiten encontrar ese rastro y castigar a los culpables. Expertos del derecho, la economía y el combate al crimen se han dado cita en un desayuno organizado por EL PAÍS con el patrocinio de Axesor para hablar de las nuevas sendas de los criminales y defraudadores y de cómo se les está combatiendo.

Lo primero es darse cuenta de que el problema es real; por suerte, las soluciones también. "La ciberseguridad es uno de los riesgos de toda industria en proceso de transformación digital, y, desde luego, eso es lo que estamos viviendo en el sector bancario", explica Joan Puig, director de Seguridad de la Información del Banco Sabadell.

"Lo que detectamos es que, mientras los entramados societarios son cada vez más complejos, las investigaciones mercantiles siguen haciéndose de forma muy manual", indica Dionisio Torre, director general de Axesor. "Hay herramientas que permiten mostrar, a golpe de clic, todos los caminos, todas las participaciones encadenadas y cruzadas. Hasta ahora, una investigación se ponía a seguir una arista, hasta que llegaba a un punto muerto y se veía obligada a empezar de nuevo. Ahora con un motor gráfico se pueden ver todos los entramados de un vistazo, y todas las líneas de investigación posibles. Es un ahorro de tiempo y recursos increíble".

En algunos sentidos, España está muy adelantada a sus socios, tanto en Europa como fuera de ella. "La Hacienda Pública española moderna se creó al tiempo que la gran revolución de la informática en los años ochenta, por lo que desde siempre ha estado en la vanguardia de la tecnología", apunta José Ignacio Alemany, socio director del bufete Alemany, Escalona & De Fuentes. "Además, España fue pionera junto con otros cuatro países en un acuerdo de intercambio automático de información, que ya se ha extendido a muchas jurisdicciones de todo el planeta".

En otras, sin embargo, queda mucho trabajo por hacer. "Hay un auge en Bolsa de la negociación algorítmica y las transacciones de alta frecuencia", explica Helena Prieto, socia de derecho penal de Garrigues. "Son operaciones que se basan en los cambios de un valor en un segundo, que son muy pequeños, pero por volumen se convierten en importantes. Y ahí España está muy mal; solo se han abierto cuatro expedientes en la CNMV. No estamos monitorizando lo que está pasando, porque está pasando".

Para Antonio López Melgarejo, jefe de la Sección Técnica de la Unidad Central de Ciberdelincuencia de la Policía Nacional, los principales problemas de ciberseguridad que se encuentran las empresas son el *ransomware* [el *software* malicioso que bloquea los ordenadores a cambio de un rescate, normalmente en bitcoin] y la captación fraudulenta de los correos electrónicos de la propia empresa para propagar estafas.

López reconoce que su unidad no puede estar a todo. "Hay que tener en cuenta que la corrupción acapara gran parte de nuestros recursos", considera. "En lo que se refiere al fraude general estamos más centrados en la aplicación de la ley que en la prevención". Y señala: "Ya estamos usando el *big data* en cosas como la distribución de recursos para la seguridad ciudadana".

Material suficiente

Material hay. "Una ley de 2010 creó el Fichero de Titularidades Financieras, donde están todas y cada una de las aperturas, cancelaciones y modificaciones de cuentas corrientes, cuentas de ahorro, depósitos a plazo y cuentas de valores, de todos y cada uno de nosotros", indica Prieto. Y la cantidad no hará sino aumentar. "La biometría es un caso interesante", apunta Puig. "No solo se trata de la que conocemos todos, la que incluye los ojos y las huellas dactilares, sino también es la llamada biometría de comportamiento; por ejemplo, la forma en la que escribimos en un teclado. Es algo que no sirve para identificar a las personas pero sí para validar que alguien es quien dice ser".

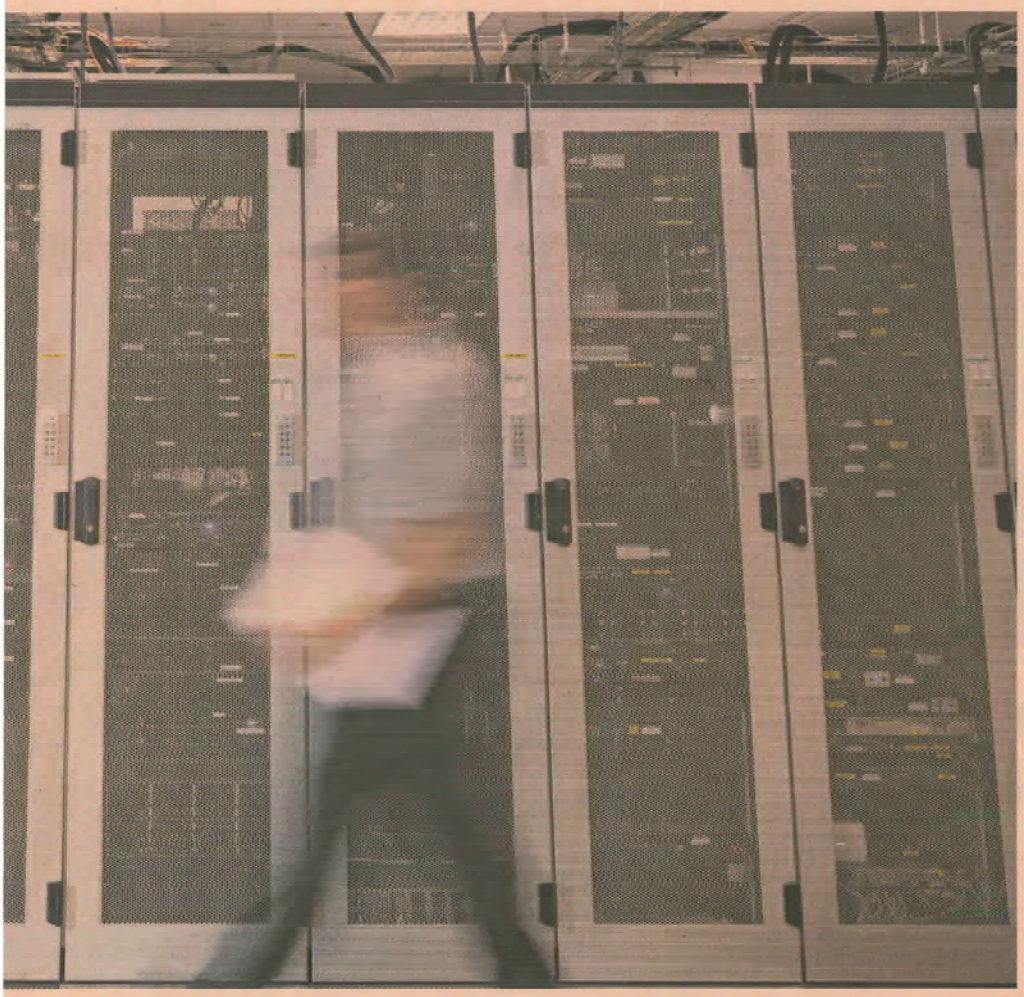
Pero toda esa información necesita ser procesada lo más rápidamente posible. "Cuando hablamos de sistemas de seguridad digital, si están orientados al cliente no puedes tardar más de dos o tres segundos", dice Puig. "La gente que paga una compra o que hace una transferencia no puede ni tiene que esperar más de eso para que se apruebe la operación. Todo esto requiere una altísima inversión en tecnología". "El factor de la urgencia hace exponencial la dificultad", apunta López.

Y el combate al crimen no tiene los recursos para seguir el ritmo de la gigantesca expansión de la sociedad de los datos. "Hay que tener en cuenta que nuestro mundo se está trasladando a lo digital", considera López Melgarejo. "En cualquier robo de coches te puedes encontrar una memoria USB, y en muchos casos para resolver un crimen hay que comprobar un perfil de Facebook. En 1995 éramos dos o tres investigadores y hoy somos más de 400, pero creo que todos los agentes necesitan esta clase de formación; somos una organización de más de 60.000 personas". No es solo un problema del sector público. "Nos vemos y nos deseamos con los profesionales que tenemos; hacen falta miles más", considera Carlos Sáiz, socio responsable del área de riesgos y *compliance* de Ecix Group. "Vamos a tener que correr".

La entrada en vigor el pasado 25 de mayo del Reglamento General de Protección de Datos (RGPD) aprobado por el Parlamento Europeo ha facilitado mucho las cosas, eliminando la necesidad de comisiones rogatorias en muchos casos. Pero la tecnología va muy por delante de la ley. "En muchos sectores, el vector de impulso es el éxito, pero en el derecho no: es el consenso, que es mucho más lento", señala López Melgarejo.

"Tecnológicamente hay muchas cosas que llevan décadas pudiéndose hacer", apunta Sáiz. "Un operador de móvil tiene la información si un usuario ha pasado en España los 183 días al año que necesita para ser residente en el país", añade Puig. "Gracias a la tecnología puede detectarse si una persona ha pasado mala noche. Eso tiene implicaciones en la seguridad y en la salud de las personas", apostilla López.

Las consecuencias éticas de la gestión de datos van más allá. "Es preocupante cómo se ha desarrollado la tecnología sin ninguna reflexión sobre sus consecuencias políticas, sociales y morales, que van más allá de la privacidad", considera Sáiz.



Los grandes centros de datos como el de la foto también conectan al crimen. MONTY RAKUSEN (GETTY)

"Creo que pecamos un poco de *buenistas*. En el momento en que cuelgas algo en Internet, tus datos ya están en otra parte y eso ya es irreversible".

Y aunque la legislación sea europea, la respuesta es nacional, lo que genera otra clase de problemas. "El principio de territorialidad es inaplicable a Internet", apunta López. "No hay un ciberderecho, y hace falta", indica Sáiz. "Lo que quiere el RGPD es que las grandes operadoras estadounidenses funcionen bajo la ley europea, pero si la incumplen en su país de origen, ¿quién les va a sancionar?" Según Prieto, "eso es lo me hace temerme que por todo el escándalo Cambridge Analytica [la compra de datos de más de 80 millones de personas a Facebook para usos políticos sin autorización] al final serán condenadas tres personas".

Pero, al final, como dijo el juez del Tribunal Supremo estadounidense Louis Brandeis, "la luz del sol es el mejor desinfectante". "Luchamos para que haya una apertura, que podamos acceder a datos no sensibles, como el de número de empleados, o resultados financieros que al final acabarán siendo publicados en el Registro Mercantil a los 18 meses", considera Dionisio Torre. "Porque, en realidad, salvo a las compañías que les va mal, ninguna tiene problema en compartir su información".

> **"Nuestro mundo se está trasladando a lo digital; en cualquier robo te encuentras una memoria USB"**

> **"Cada país desarrollado tiene su paraíso fiscal de confianza que le sirve de cloaca y refugio de capitales"**

No solo las empresas privadas son problemáticas. "Hay también mucho desconocimiento de la Ley de Reutilización de Datos del Sector Público", continúa Torre. "Aunque también hay organismos, como el Catastro, cuya transparencia es modélica; salvo algunos datos realmente sensibles, como el nombre de los propietarios, ahora puede encontrarse el número de expediente y la calificación de cualquier terreno en España".

Todas estas herramientas son importantes porque, como apunta Alemany, "no nos tenemos que engañar: no va a dejar de haber delitos". "Hay que tener en cuenta que territorialidad es soberanía", prosigue. "Cada país desarrollado tiene su paraíso fiscal, su cloaca donde van a parar los fondos que tienen que lavar y esto va a pasar mientras haya países soberanos". "Vamos a ver el surgimiento de paraísos cibernéticos", confirma López.

El responsable policial explica que aunque la tecnología está avanzando a marchas forzadas, la principal herramienta de la justicia es la torpeza de los propios criminales. "En una de nuestras últimas operaciones contra el blanqueo, conseguimos detener a alguien porque había usado una firma de bitcoin que conocíamos. Al final se trata de esperar a que alguien cometa un error, pensar que no todos van a ser tan audaces y que nosotros vamos mejorando con el tiempo".

Eso es por lo que, para Torre, una de las más importantes contribuciones que puede hacer la empresa privada a la ciberseguridad es "conectar ecosistemas reputacionales": que las empresas e instituciones que tengan plena confianza creen sistemas comunes fiables. "Certificar los procesos es algo deseable, porque incentiva la autorregulación", considera Alemany. "Las empresas que desean un marchamo de buenas prácticas pueden buscarlos por una cuestión reputacional".

Sin embargo, ahora mismo las empresas que cumplen con la legislación no reciben ningún incentivo por hacerlo. "Un código de buenas prácticas no está dentro de la ley", indica Alemany. "Hay que tener en cuenta que la autorregulación obliga a desviar muchos recursos del propio negocio", apunta Prieto. "El adherirse a un código de buenas prácticas podría servir como descargo de responsabilidad societaria".

PARTICIPANTES

● **Dionisio Torre**
● Director general de Axesor
"Hasta ahora, una investigación llegaba a un punto muerto y se veía obligada a empezar de nuevo. Ahora con un motor gráfico se pueden ver todos los entramados de un vistazo (...) Es un ahorro de tiempo y recursos increíble"

● **José Ignacio Alemany**
● Socio director de Alemany, Escalona & De Fuentes
"La Hacienda Pública española moderna se creó al tiempo que la gran revolución de la informática en los años ochenta, por lo que desde siempre ha estado en la vanguardia de la tecnología"

● **Helena Prieto**
● Socia de Derecho Penal de Garrigues
"Hay que tener en cuenta que la autorregulación obliga a desviar muchos recursos del propio negocio. El adherirse a un código de buenas prácticas podría servir como descargo de responsabilidad societaria".

● **Antonio López Melgarejo**
● Jefe de la Sección Técnica de la Unidad Central de Ciberdelincuencia de la Policía Nacional
"Las autoridades educativas deberían tener en cuenta, a la hora de enseñar a los niños el conocimiento del medio, que ese medio en el que viven también incluye el ciberespacio".

● **Joan Puig**
● Director de Seguridad de la Información del Banco Sabadell
"Un operador de móvil tiene la información si un usuario ha pasado en España los 183 días al año que necesita para ser residente en el país"

● **Carlos Sáiz**
● Socio responsable del área de riesgos y 'compliance' de Ecix
"Es preocupante cómo se ha desarrollado la tecnología sin ninguna reflexión sobre sus consecuencias políticas, sociales y morales, que van más allá de la privacidad"