



Primer Congreso nacional antifraude celebrado este jueves en Madrid Manuel Hernández Urquijo

Cómo combatir el fraude actual: sofisticado y transnacional

- Los expertos coinciden en el primer congreso nacional antifraude, celebrado este jueves en Madrid, en la importancia de implantar una cultura de cumplimiento en las organizaciones.

5D

ANA VELA MOURIZ / IRENE RUIZ DE VALBUENA

9 FEB 2018 - 14:08 CET

El primer Congreso Nacional Antifraude, celebrado este jueves en Madrid y organizado por la World Compliance Association junto con la Fundación Universitaria Behavior & Law puso de manifiesto que la lucha contra el fraude es una preocupación muy extendida. La globalización, el avance de las tecnologías y el aumento de intercambios comerciales han fomentado la proliferación de conductas corruptas y fraudulentas, hasta el punto de que sean los únicos delitos que han aumentado exponencialmente en 2017.

El encuentro contó con muchos expertos, cuya finalidad fue aclarar aspectos propios del fraude y anticiparse a las nuevas tendencias, con el propósito de ofrecer [herramientas válidas para que las empresas puedan prevenir](#), detectar y contrarrestar las amenazas de fraude.

El Congreso abrió con la exposición de José Luis Olivera Serrano, director del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), que explicó cómo han evolucionado los tipos de fraude desde el timo de la estampita hasta las cartas nigerianas, o métodos más sofisticados que usan las nuevas tecnologías para operar. Además, en su opinión la definición más exacta de lo que es el fraude, es la dada por Transparencia Internacional: "el abuso del poder público para facilitar o beneficiar al poder privado". En cuanto a la evolución del fraude destacó que desde la reforma del Código Penal en 2010 en la que se implantó la responsabilidad penal de las personas jurídicas, cada vez el ataque es menos individual y más corporativo. Todo ello, obliga a las empresas a crear una cultura organizativa de cumplimiento, aplicando manuales de buenas prácticas y promocionando valores éticos y de transparencia, para prevenir la comisión de delitos y sus consecuencias. Los tres pilares de estos manuales son: la prevención, detección y corrección.

A continuación, Daniel Faura, presidente del Colegio de Censores Jurados de Cuentas de Cataluña, enseñó el árbol del fraude con los delitos económicos más frecuentes, y explicó cómo es el perfil del defraudador: de entre 31 y 55 años, entre un 70-80% hombres, 65% empleados de la propia organización, con estudios universitarios, espabilado, ingenioso, falso, manipulador, mentiroso, seductor, dominante e inquisitivo. Con todo ello estableció la siguiente ecuación:

Volumen: + edad + antigüedad + responsabilidad = ¡+importe defraudado!

Ofreció también interesantes datos de un estudio de ACFE sobre los tipos de fraudes que serán más habituales en 2018: el 60% ciberataques, el 44% uso de criptomonedas, el 43% robo de identidad de consumidores.

Para concluir su exposición lanzó una interesante reflexión, sobre el problema de base del fraude: la habitual tolerancia que en España los empresarios y de los ciudadanos en general, tienen frente a las corruptelas. Es decir, que está socialmente aceptado colarse en la lista de espera de la sanidad si se conoce a alguien en la Administración o empadronarse en un lugar distinto para conseguir entrar en un determinado colegio.

Por su parte, Juan Antonio Frago, Fiscal de delitos económicos, insistió en que en España no hay una política real de represión de los delitos de corrupción. En su opinión, los jueces no cuentan con una formación específica en este tipo de delincuencia compleja, ni se han habilitado juzgados especializados para esta materia como sí se ha hecho por ejemplo para las reclamaciones por cláusulas suelo. En su intervención también abordó los cambios legislativos que, desde su punto de vista, deben producirse para combatir el fraude como reunificar los delitos para poder aplicar la reincidencia a ellos, una proporcionalidad en las penas, medidas cautelares

más severas y en tiempo razonable para recuperar el dinero o periciales contables que no se dilaten en el tiempo por problemas de distintas regulaciones en cada comunidad autónoma. Asimismo, Frago reclamó más medios y formación para las Fuerzas y Cuerpos de Seguridad del Estado y más coordinación entre cuerpos, la necesidad de un estatuto del compliance officer y del whistleblower, e incentivar económicamente al trabajador que demuestre que se ha cometido un fraude dentro de la organización.

Juan José Matías González, responsable de Prevención Fraude y Blanqueo Capitales en ASNEF, destacó que España es el país de la Unión Europea donde se producen más robos de identidad por internet. También reclamó poder acceder a los ficheros de las nóminas de los miembros de la Administración para poder detectar anomalías y a las pensiones, que no constan en el fichero que ofrece la TGSS.

Por otro lado, Albert Salvador, secretario General de la World Compliance Association, señaló la importancia de establecer controles en las corporaciones porque tienen un efecto alerta y disuasorio. Si se sabe que los hay, se cometen menos fraudes. Ofreció un decálogo de cómo diseñar controles antifraude y qué habilidades se necesitan para crear y tratar esos controles y su conclusión fue que lo importante no es generar muchos controles, sino los suficientes para que se puedan tratar, de lo contrario son ineficaces.

El Secretario de la asociación española de empresas contra el fraude (AEECF), Pablo Pascual, insistió en su ponencia en las implicaciones de la inteligencia artificial en la toma de decisiones, ya que, según expuso, existe un cierto "miedo a lo que puedan hacer los robots". Es por ello, que el reglamento europeo de protección de datos limita en su artículo 22 la toma de decisiones individuales automatizadas así como la elaboración de perfiles. De manera que, todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, que incluya la elaboración de perfiles. Y sólo se podrá hacer en los casos en los que sea absolutamente necesario elaborar el perfil para la ejecución de un contrato que, además, ha de estar permitido por norma que garantice el cumplimiento de los derechos, libertades e intereses legítimos del interesado y cuente con su consentimiento. En definitiva: "Con la legislación actual las máquinas no pueden actuar solas, es necesario que haya una persona al menos al final del proceso o en su supervisión". Sin embargo, en los supuestos de prevención del fraude no será necesario el consentimiento expreso del interesado, debido al interés legítimo que hay detrás, lo cual no impide que se tenga que cumplir con las demás obligaciones de protección de datos, como son: informarle del tratamiento de sus datos y que tenga los derechos a intervención humana y a recurrir decisión.

Acto seguido, Giovanni Castellanos, VP de Ventas y Mercadeo de Plus Technologies, comentó cómo el fraude impacta negativamente en la experiencia de cliente, hasta el punto de que el 36% deja de usar el producto después de un fraude. Asimismo, insistió en que el fraude ha llegado a

tal altas cotas que hoy día se puede hablar del Faas (fraude as a service), empresas que ofrecen el fraude como un servicio cualquiera.

A continuación, Manuel Palma Escobar, Jefe de Servicio de la División de Crimen Organizado, expuso cómo el Big Data puede ser la gran herramienta para luchar contra el fraude, y lo importantes que son los modelos de inteligencia de las empresas y análisis de riesgos y los servicios de seguridad. El Big Data aplicado a la seguridad puede ser la solución contra la criminalidad organizada, junto con una combinación de información/inteligencia de las Fuerzas y Cuerpos de Seguridad del Estado y las empresas privadas y públicas.

En su intervención, Mariano Paradell, CEO en Grupo Paradell y detective privado, destacó que en su opinión, en España somos demasiado confiados y sólo reaccionamos cuando el daño ya está hecho y que es más cara la reacción que la prevención. "En ocasiones se tarda un año en detectar el fraude en una compañía, lo que supone grandes pérdidas económicas y reputacionales" apuntó. Asimismo, señaló que es fundamental que las empresas se conciencien de ello e implanten una cultura ética, controles, auditoría interna, canal de denuncias y las due diligence, para prevenir el fraude.

Miguel Toledo, socio director en T & T Abogados aprovechó su ponencia para resaltar la importancia de que todos los controles que una empresa implante sean conocidos por sus trabajadores. La formación y la información de los empleados es fundamental para que esos controles funcionen y concluyó con tres máximas: "las cosas se hacen antes, conjuntamente trabajador y empresario y las medidas vienen a beneficiarnos a todos y no a fiscalizar a nadie."

Francisco Enrique González Iturralde, comandante de la Guardia Civil, Unidad Técnica de Policía Judicial (UTPJ), explicó que su trabajo ante la comisión de fraudes consiste en elaborar informes de patrimonio que se presentan al juez, uniendo varias técnicas: la explotación de bases de datos, la actividad operativa policial tradicional, el análisis de información económico patrimonial y la cooperación internacional. Además se encargan también de la recuperación de activos provenientes de actividades fraudulentas.

Enrique Solana, CEO en FOXid, quiso hacer hincapié en lo fácil que resulta en la actualidad el robo de identidad para cometer fraudes, aunque añadió que "cualquiera puede entrar en internet y comprar un DNI falso". Para él, la solución para combatir el fraude es aplicar la inteligencia artificial para la identificación y verificación de minucias unida al big data.

Muy práctica fue la exposición de Faustino Aparicio Ruiz, comisario del Cuerpo Nacional de Policía y Jefe de la Brigada Central de Inteligencia Financiera, que comenzó destacando que en el último año la comisión de fraudes se ha disparado mientras que la de los demás delitos han bajado. También explicó cómo la Comisión de inteligencia contra el blanqueo de dinero está trabajando junto con EUROPOL para dar entrada al sector privado en la persecución del fraude. De manera que cada vez que se produzca un fraude en la Unión Europea, el sector privado

pueda tener conocimiento inmediato. Así, la empresa será sujeto activo en la lucha contra el fraude y podrá implantar medidas, que en su opinión es lo más importante.

Por la tarde, Jorge Jiménez, director del Máster de Análisis de Conducta de Fraude y del Máster en Perfilación Criminal SAFE; Rafael López, presidente de la Fundación Universitaria Behavior & Law; y Antonio Domínguez, director del Instituto de Análisis de Conducta Antifraude, fueron los encargados de explicar cómo las técnicas de análisis de conducta, que detectan la mentira, pueden aplicarse en el ámbito empresarial, siendo muy útiles en recursos humanos para saber si las personas son "de fiar".

Por su parte, Juan Enrique Soto, profesor de la Fundación Behavior & Law, expuso cómo las técnicas de interrogatorio policial pueden aplicarse a la entrevista de seguridad del personal de una empresa.

Por último cerrando el encuentro, Leticia Perinat, directora del Máster de Pericia Caligráfica y Documentoscopia de la UDIMA, explicó, con casos reales, cómo la pericial caligráfica y el uso de la documentoscopia pueden usarse para detectar falsos documentos como DNI, cheques, etc, usados para cometer fraudes.

En conclusión, la mayoría de los ponentes estuvieron de acuerdo con el refranero popular: "más vale prevenir que lamentar". Esto solo se consigue implantando una [cultura de cumplimiento en las organizaciones](#), manuales de buenas prácticas que promocionen valores éticos y de transparencia, aplicando estos tres pilares: la prevención, la detección y la corrección.