RESUMEN DE LA JORNADA ORGANIZADA POR LA LECE – DELOITTE SOBRE GEOPOLÍTICA, CIBERRESILIENCIA Y FRAUDE EN PAGOS: UNA MIRADA CONJUNTA AL FUTURO DIGITAL

Deloitte y el **Comité Español de la LECE** celebraron una jornada en Madrid el pasado 23 de octubre dedicada a tres de los grandes desafíos del mundo actual: la geopolítica, la ciberresiliencia y el fraude en pagos. Tres ejes interconectados que reflejan la compleja encrucijada en la que se encuentra hoy la economía global y, en particular, el sistema financiero europeo.

Bajo el título "Geopolítica, Ciberresiliencia y Fraude de Pagos", el seminario reunió a expertos del ámbito institucional, tecnológico y financiero para analizar, con rigor y profundidad, cómo estos fenómenos impactan en la estabilidad, la confianza y la soberanía digital de Europa.

El acto se inició con unas palabras del **Presidente del Comité Español de la LECE, Sr. Francesc Homs**, que enmarcó la Jornada dando respuesta al porqué de la organización de este evento. Palabras que compartió con el **socio de Ciberseguridad - Technology & Transformation de Deloitte Sr. Eduardo Ferrero**, quien puso de manifiesto el interés de su organización en todas las cuestiones relativas a la ciberseguridad.

Durante la apertura, con el **responsable de Digital Finance de la Comisión Europea, Mattias Levin**, y el desarrollo de las mesas, se destacó la necesidad de abordar los retos digitales desde una perspectiva compartida y con una visión estratégica de largo plazo. La jornada permitió constatar que la ciberresiliencia ya no es solo un asunto tecnológico, sino que constituye un elemento geopolítico esencial.

En el primer bloque, centrado en la ciberseguridad, el mismo **Levin**, junto con **Pablo Martín, de Deloitte; Llorenç Malo, de Caixabank y Joan Puig, del Banc Sabadell**, moderados por **Javier Arias, presidente de la LECE central**, resaltaron que los ciberataques han dejado de ser exclusivamente criminales para convertirse en instrumentos de influencia estatal, lo que exige reforzar la cooperación transfronteriza y avanzar hacia marcos regulatorios unificados en el seno de la Unión Europea. La ciberseguridad es hoy la base de la seguridad económica y soberana de Europa.

La ciberresiliencia ya no es solo un asunto tecnológico, sino un elemento geopolítico esencial para la soberanía digital de Europa

El segundo bloque del seminario, centrado en el fraude en pagos, puso de manifiesto que este es uno de los principales campos de batalla del mundo digital. **Carlos Sanz Eluengo, del Banco de España; Paola Papp, de Frontier Economics; Víctor López Gracia, de Banco Sabadell; Christian Castro, de Caixabank y Gonzalo Díaz Oliver, de Deloitte**, moderados por **Alejandro Negro, de Cuatrecasas**, coincidieron en que la confianza del consumidor es el pilar de la economía digital, y que su preservación exige una colaboración total entre bancos, 'fintechs', reguladores y consumidores. La prevención del fraude,

recordaron, no puede ser una tarea aislada: es una responsabilidad colectiva que requiere innovación constante y un intercambio ágil de información en tiempo real.

A lo largo de la jornada también se destacó el papel de la tecnología como catalizadora y solución. Si bien es fuente de vulnerabilidad, es a la vez la herramienta más poderosa para la defensa y la anticipación. Desde el uso estratégico de la inteligencia artificial para detectar patrones de ataque hasta la gestión del riesgo geopolítico, la tecnología se consolida como la base de la resiliencia futura de Europa.

La prevención del fraude digital es una responsabilidad colectiva que requiere innovación constante y colaboración entre bancos, fintechs, reguladores y consumidores

En las conclusiones finales, **Javier Arias** remarcó el valor del diálogo y la colaboración entre sectores. También incidió en que el conocimiento compartido, las ideas generadas y los lazos fortalecidos hoy deben servir como motor de una era digital más segura y próspera.

El espíritu de la jornada, marcada por el intercambio de visiones y la búsqueda de soluciones comunes, refuerza el compromiso de la LECE y de Deloitte con el progreso económico europeo, la innovación y la seguridad digital en un entorno global cada vez más complejo.

De todas las intervenciones que tuvieron lugar en la jornada se podría resumir que se trataron las siguientes cuestiones:

1. **En tecnología y ciberresiliencia:**

- La necesidad de gestionar riesgos de tecnología, sistema y continuidad del servicio: los proveedores de servicios de pago y entidades financieras deben prepararse no solo para prevenir incidentes, sino para responder, recuperarse y mantener la operativa ante interrupciones. Que la Regulación se ajuste a las necesidades.
- Interdependencia y cadena de suministro de TI/ICT: los proveedores de servicios financieros dependen de múltiples terceros (plataformas, APIs, cloud, proveedores de servicios de infraestructura) que también deben ser gestionados para garantizar la resiliencia. Se reclama más coordinación.
- Formación, conciencia y cultura de seguridad: numerosas pymes y negocios tienen desconocimiento sobre ciberataques y fraude digital.
- Regulación emergente: por ejemplo el Digital Operational Resilience Act (DORA) imponiendo un marco uniforme para instituciones financieras, con obligaciones de gestión de riesgos de ICT, pruebas de resiliencia, reporte de incidentes.
- Coordinación transfronteriza y seguimiento de incidentes: los sistemas de pago están muy interconectados en la UE, lo que implica que un incidente grave puede propagarse rápidamente entre países y entidades.
- Promover una mayor coordinación de todos los agentes que Intervienen en el proceso. Falta un “Espacio” para compartir análisis y diseñar las medidas de Seguridad a

proponer para poder definir como se construye el futuro. La Comisión Europea debería promover una mayor coordinación entre los agentes del mercado , Entidades Financieras y Estados.

- La UE debe impulsar una estrategia para crear empresas europeas proveedoras de tecnología, para reducir la elevada dependencia actual de proveedores americanos y chinos.

2. En fraude digital en los pagos:

- El fraude mediante pagos sigue siendo una de las principales preocupaciones para los consumidores en la UE: la European Banking Authority (EBA) lo ha identificado como el problema más importante para los consumidores.
- Evolución de técnicas de fraude: phishing, ingeniería social, fraude "autorizado" (donde se engaña al pagador para que haga el pago), fraude "card-not-present" (CNP), pagos a cuentas de fraudadores, etc.
- Autenticación reforzada del cliente (Strong Customer Authentication, SCA): ha tenido impacto positivo en reducir ciertos tipos de fraude. Seguir reforzando la prevención coordinada.
- Responsabilidad y reparto de pérdidas: la asignación de quién soporta la pérdida por fraude (usuario, banco, proveedor de pagos) es un tema clave, y pueden existir vacíos de protección para el consumidor. Incrementar la coordinación para que todos los Bancos actúen de la misma forma
- Falta de protección uniforme para usuarios en nuevos métodos de pago (por ejemplo pagos instantáneos, nuevos proveedores de servicios de pago) lo que genera riesgo de confianza.
- Si los sistemas de detección de fraude o las infraestructuras de pago fallan, puede producirse interrupción de servicios, afectación de liquidez, pérdida de confianza en los usuarios.
- Ante pagos instantáneos (real-time) y servicios digitales, el margen de reacción ante incidentes es más pequeño: se requiere mayor automatización, monitorización continua y arquitecturas resilientes.
- Más coordinación entre Entidades Financieras. Simplificación de Regulación

3. Particularidades en el entorno UE:

- Marco regulatorio propio: por ejemplo la Directive (EU) 2019/713 sobre la lucha contra el fraude de medios de pago no en efectivo.
- El mercado de pagos paneuropeo (SEPA, pagos instantáneos, PSPs, bancos, fintech) hace que las normativas tengan que contemplar la operativa transfronteriza, interoperabilidad, así como coordinación entre autoridades de distintos Estados miembros.
- La digitalización creciente de los pagos amplía la superficie de riesgo: más pagos online, más plataformas, más TTP (terceros prestadores) implicados, lo que exige adaptarse.

4. Cuestiones comunes, interrelación entre ciberresiliencia y fraude:

- La ciberresiliencia robusta contribuye a reducir el fraude: si un proveedor tiene una arquitectura fuerte, controles, monitorización, incident response, recuperación, ello mitiga los vectores de ataque que pueden originar fraude.
- Del mismo modo, los eventos de fraude grandes pueden generar interrupciones, daño reputacional, pérdidas operativas, lo cual pone de relieve la necesidad de resiliencia.
- La obligación de reporte de incidentes, la cooperación entre entidades, el intercambio de información sobre amenazas y vulnerabilidades son factores críticos.
- La supervisión regulatoria se está endureciendo tanto para la resiliencia operacional (por ejemplo DORA) como para el fraude en pagos. El cumplimiento regulatorio ya no es opcional.

5. Principales retos y preguntas:

- Asegurar que los pequeños proveedores de servicios de pago (PSP) o fintechs puedan cumplir los elevados estándares de resiliencia y antifraude sin incurrir en costes prohibitivos.
- Armonizar la protección al consumidor en todos los Estados miembros, garantizando que los usuarios tengan derechos efectivos frente al fraude y los incidentes de pago.
- Garantizar que los proveedores de servicios de pago implementen una evaluación de los riesgos de fraude en tiempo real (o casi) y puedan reaccionar ante nuevas formas de fraude (ingeniería social, aplicaciones maliciosas, deepfakes, etc.)
- Manejar la responsabilidad y el reparto de pérdidas de manera que no se genere desincentivo para que los bancos/prestadores colaboren en prevención. Cambios en la futura regulación de pagos podrían incentivar el “blame shifting”.
- Promover una mayor seguridad de la cadena de suministro de TIC, de los servicios en la nube, los terceros y los proveedores de infraestructura, sin perder agilidad.

6. Marco regulatorio relevante en la UE:

- Digital Operational Resilience Act (DORA): establece un conjunto uniforme de requisitos para la resiliencia operativa digital de entidades financieras.
- La Directiva (UE) 2019/713 sobre la lucha contra el fraude de medios de pago no en efectivo.
- Próximo/regulación en curso: Cyber Resilience Act (CRA) para productos con elementos digitales, lo cual también afecta al entorno tecnológico de pagos.
- Normas de autenticación fuerte del cliente (Strong Customer Authentication, SCA) en el marco de la Payment Services Directive 2 (PSD2), que han demostrado efectividad en reducción de fraude.