*Transacciones electrónicas seguras: aplicación de las normas de la UE*

El Reglamento eIDAS, y principalmente el principio de reconocimiento mutuo, ha sido un gran paso para fomentar un Mercado Único de servicios digitales de confianza.

El Reglamento dio respuesta a una demanda que se ha demostrado creciente y muy necesaria: la confianza en las transacciones electrónicas, sobre todo de la identidad de quien está detrás de la actividad on-line. En definitiva, fomentar la creación uno de los elementos imprescindibles para el desarrollo del Internet del Valor.

Posteriormente otras normas también han incidido en la necesidad de aplicar herramientas de identidad segura en ciertos ámbitos sectoriales. El ejemplo más cercano es la PSD2 en el ámbito de los pagos digitales que ha significado la exigencia de la identificación segura mediante doble factor de autenticación (SCA) para permitir el desarrollo del mercado único europeo de pagos digitales, reduciendo los frenos asociados al fraude en las operaciones de pago, es decir, la incertidumbre y la inseguridad asociados a la identidad de los ordenantes de los pagos digitales.

La experiencia adquirida en estos años permite reflexionar sobre las luces y las sombras asociadas a algunos servicios de confianza, y en especial su implementación y difusión en algunos ámbitos concretos. Incluso permite señalar una oportunidad estratégica para la industria digital desarrollada en Europa, de modo que juegue un papel clave y central como garante de esa identidad digital segura necesaria para el desarrollo del Internet del Valor. Aprovechar esta oportunidad significaría contribuir al progreso de la industria digital en Europa en los temas de identidad digital segura, sirviendo de ejemplo a otras áreas geopolíticas.

Y de la experiencia en estos años de aplicación del Reglamento eIDAS se derivan dos aspectos: por un lado, la necesidad de que **las autoridades europeas lideren y financien la creación de las guías de uso con los estándares adecuados a los usuarios europeos sobre las soluciones proporcionadas** por la industria en Europa y, por otro lado, la necesidad de prestar **una mayor atención a la usabilidad y la adopción de las soluciones tecnológicas de identidad digital segura**.

Comenzaremos comentando la necesidad de proactividad en **guías a nivel europeo más** que la actual adaptación. El ejemplo más cercano son los recientes acontecimientos relacionados con la aplicación de la SCA de la PSD2 en los pagos digitales europeos, que han puesto de manifiesto la dificultad de que una industria como la financiera adopte de manera individualizada a nivel empresa, un nivel uniforme de exigencia mayor en cuanto a la seguridad de la identidad. Probablemente el desconocimiento técnico en muchos operadores financieros y en algunos reguladores han llevado a un retraso evidente en las guías de la EBA y, consecuentemente, en la implementación de las tecnologías de SCA exigidas por la normativa PSD2. Como consecuencia de esa falta de foco, la fecha límite de 14 de septiembre 2019 establecido en la PSD2 ha sido incumplido de manera generalizada y ha obligado a la EBA a aconsejar un periodo de "flexibilidad supervisora" hasta diciembre de 2020.

Es un hecho en octubre 2019 que ya existe tecnología disponible para garantizar el cumplimiento de la normativa en tiempo y forma. De hecho, las entidades financieras de algunos países

europeos (los países nórdicos) ya han estado aplicando el nivel requerido de seguridad en la autenticación a través de tecnologías como las basadas en SIM[1].

Esas tecnologías que permitirían cumplir los requisitos de SCA de la PSD2 pueden ser aportadas de forma inmediata e interoperable (estándar abierto a nivel mundial). En concreto a través de servicios basados en el estándar Mobile Connect, desarrollado por la GSMA a nivel global y que ya está implementado en muchos de los países europeos y, por tanto, disponible para los usuarios que disponen de teléfono móvil (es decir, la práctica totalidad de los ciudadanos europeos).

Sin embargo, la falta de guía de las instituciones europeas (la Comisión UE, la EBA, etc) en la promoción de la adopción de este tipo de tecnología ha dejado escapar una oportunidad para proporcionar un escenario mejor en el que las instituciones financieras europeas pudiesen dar cumplimiento en plazo a la normativa PSD2.

Sería necesario que la Comisión Europea analizase el impacto que tiene el retraso en la adopción por los sectores económicos de soluciones de identificación seguras y, a la vista de los resultados, hiciese las propuestas necesarias para apoyar la difusión y adopción de soluciones (SIM Based como las basadas en el estándar tecnológico Mobile Connect).

Por otro lado, tenemos necesidad de que las hojas de ruta tengan muy en cuenta **la usabilidad de las soluciones** y, por tanto, su facilidad de adopción. Si las soluciones son muy robustas, pero poco usables los ciudadanos no las adoptarán y el nivel de seguridad será menor del deseable. En este sentido tenemos ejemplos de sectores en los que se han desarrollado soluciones tecnológicas muy seguras para los servicios de confianza digitales, pero poco usables y, por tanto, escasamente adoptados por los usuarios. Este es el caso de servicios de identificación para servicios eGovernment como el eDNI español o el sistema PIN Cl@ve. Ambos son sistemas muy seguros (certificados como servicios de confianza a nivel UE) pero tan complejos de usar (requieren la instalación de software propietario y/o la disponibilidad de un lector) que no son apenas utilizados por los ciudadanos. En el caso de los servicios públicos se une además la complejidad de la coexistencia de diferentes niveles geográficos de autoridades públicas (en el caso español coexisten niveles de Administración estatal, regional y local) cada una soberana en la adopción de mecanismos de identificación digital segura (lo que conlleva ulterior fragmentación y falta de interoperabilidad). Por dar una cifra, según la web del Ministerio del Interior, el eDNI se puede usar en unas pocas decenas de Gobiernos locales, cuando en España son más de 8.000 los Gobiernos locales en los que debería poder utilizarse para que realmente fuese una solución usable de identidad digital.

Para solucionar estos problemas sería necesario que la Comisión Europea realizase un **análisis de impacto del uso real** (no sólo de disponibilidad) de las soluciones de servicios de confianza digital a nivel de los servicios eGovernment (no sólo a nivel de Administración nacional, sino también regional y local) y de los beneficios sociales que disfrutarían los ciudadanos europeos si dispusieran de un mecanismo de identificación digital segura en su línea de teléfono móvil basado en un estándar interoperable. Este es el caso que ha seguido el Gobierno francés con France Connect y que podría extenderse rápidamente a países en los que los operadores móviles ya tienen implementado ese estándar, como es el caso español.

[1] Ya vez superado el problema de capacidad de la SIM que señalaba ENISA en la pagina 32 de su documento de 2013 titulado **eID Authentication methods in e-Finance and e-Payment services - Current practices and Recommendations**

Adicionalmente el desarrollo de una **solución de identidad digital segura basada en tecnologías SIM Based** podría tener muchas aplicaciones en campos que necesitan de soluciones como los siguientes:

- **Control de acceso de menores a contenidos on-line para adultos** (ejemplo gaming). El acceso de menores a contenidos que pueden ser legales pero que están destinados a mayores de edad es un tema que genera creciente preocupación. El requerimiento de una identidad digital segura (de la que, respetando el anonimato, puedan consultarse determinados componentes como la exigencia de mayoría de edad) aportaría seguridad al desarrollo de negocios como el gaming, respetando del cumplimiento de la normativa de protección de menores.

- **Reducción de niveles de fraude en actividades como la reventa on-line de tickets de espectáculos.** La regulación de la reventa de entradas de espectáculos ha quedado desfasada en un contexto en el que gran parte de la venta y la reventa se realiza on-line. La combinación de la exigencia de identidad digital segura (fácil, usable y universal) y tecnología blockchain podría dar una salida al desarrollo fluido del negocio, evitando posibles problemas de fraude al consumo que puedan producirse.