>> Jorge Dávila

European Fashion Victims

Las sociedades se parecen mucho a los ciudadanos que las componen, por lo que tienen tendencias a presentar las mismas debilidades que éstos. Al igual que existen modas periódicas que mantienen en marcha el motor de la producción y del despilfarro a nivel de los ciudadanos de a pie, en las decisiones de los estados y estructuras supranacionales también pueden estar cautivadas por estériles modas. La Unión Europea no es ajena a esta debilidad y también sigue sus modas. Dado el impacto que este proceder tiene en nuestras economías y en nuestro deambular histórico, conviene que echemos un vistazo a cuáles son algunas de las "modas" –European Fashion Victims[1]– actualmente en este rincón el mundo.

El 9 de noviembre de 1989 la Democracia occidental comenzó su lento declinar, y todavía hoy continua en el mismo sentido. En esa fecha, cae el denominado Muro de Berlín[2] que se instaló el 13 de agosto de 1961 para separar la zona de la ciudad correspondiente a la República Federal de Alemania (RFA), Berlín Oeste, de la capital de la República Democrática Alemana (RDA), Berlín Este. Ese muro físico y administrativo fue el símbolo más conocido de la Guerra Fría y de la división de una Alemania vencida. Por una parte, lo llamaban "Muro de Protección Antifascista" (Antifaschistischer Schutzwall), mientras que los medios de comunicación y parte de la opinión pública occidental se referían a él como Muro de la Vergüenza (Schandmauer).

La idea de ese muro erigido por la RDA era impedir la migración masiva de ciudadanos del este hacia occidente. En aquellos años y hasta 1989 la Europa continental era importante porque en sus campos se desarrollaba una nueva guerra en la que no eran armas balísticas y explosivas lo que se utilizaban, sino conceptos y economías.

Por una parte, el bloque pro soviético se deshacía en elogios al sistema económico programado socialista y de lo bien tratados que estaban todos sus trabajadores. En esa utopía oriental (decía que) se había desterrado la desigualdad y a cada cual se le trataba según sus méritos y sus necesidades. Sin embargo, prácticamente todo venía marcado por el estado, único agente en esa sociedad de (supuestos) pares.

Por otra parte, teníamos a los ciudadanos occidentales liberados del nazismo, pero sometidos a un capitalismo económico que fomentaba las desigualdades y ensalzaba la plutocracia. Ambos bloques intentaban sublevar a los ciudadanos del otro bloque; los soviéticos intentaban sublevar a los obreros y ciudadanos oprimidos, y los de occidente hablaban de la Democracia y de la capacidad y posibilidad de cualquiera para elegir "libremente" su destino. Desde aquellos años la Democracia, entendida como la capacidad para organizar y desarrollar, (supuestas) elecciones colectivas del futuro por sufragio directo e igualitario, ha sido utilizada como emblema de Europa, y como arma arrojadiza (junto a la defensa de los derechos humanos) ante cualesquiera iniciativas totalitarias, de las que hay hoy en día existen muchas (Rusia, China, India, etc.).

Una Civilización Europea

En el crisol de esa batalla se fraguó la idea de lo que hoy llamamos Europa, aunque sus orígenes quizás realmente habría que buscarlos en el Imperio Romano y sus interacciones con los "bárbaros" del norte y del este de nuestro continente. Toda esa historia da lugar a lo que podría considerarse una Civilización Europea ahora basada más en "valores" morales, éticos y culturales que en la potencia económica o militar, propiamente dicha.

Caído el muro, pierden eficiencia los argumentos de la guerra fría, la organización social y económica soviética prácticamente nadie la defendería hoy en día, pero tampoco la **democracia** y la **sociedad de consumo** con la que se amilanó durante tiempo a los ciudadanos soviéticos. Cayó el muro de Berlín y Alemania se reunificó, la idea de una Unión Europea de países soberanos se siguió repitiendo tenazmente, pero desde hace cuatro décadas lo que está creciendo en el escenario de la antigua guerra fría es el autoritarismo y grupos claramente antidemocráticos[3].

Siguiendo el modelo de que las Civilizaciones nacen, crecen y mueren[4] en función de muchos factores organizativos y culturales pero, sobre todo, de factores económicos, ahora Europa debe encontrar cómo desarrollar peculiaridades que la hagan atractiva y poderosa si quiere seguir ocupando algún puesto en el teatro geoestratégico del planeta.

Dado que Europa son valores sociales y organizativos, y que es un mercado con bastante gente con un nivel de vida envidiable (y envidiado), no tiene fácil competir en escenarios basados en el trabajo barato y la abundancia de mano de obra. Tampoco tenemos una economía centrada en la guerra (eso sólo trae penuria a sus habitantes y riqueza a sus dirigentes) por lo que poco o nada podemos imponer los europeos a otros.

Los eWallets que cada estado miembro desarrolle tendrán en común ser contenedores digitales, probablemente cifrados, que guarden en su interior los documentos públicos que constituyen los certificados digitales de atributos. Su uso, es decir, la extracción e inclusión de documentos en ellos, requerirán algún tipo de autenticación segura por parte del usuario y ¿cómo se va a conseguir eso?

La Unión Europea se encuentra en una encrucijada esencial, en la que todos, muy nerviosos, intuyen que, si no se hace algo y no se hace bien, en unas cuantas generaciones nadie se acordará de lo que hoy es nuestro día a día.

En esa encrucijada las instituciones europeas parecen haber optado por la generación de "valor añadido" y hacer que haya que contar con Europa para la producción y por un desarrollo de servicios valiosos para futuros y presentes ciudadanos/consumidores exigentes.

Lo que ocurre es que esa decisión no sé si está suficientemente madurada puesto

[1] Ver https://es.wikipedia.org/wiki/Fashion_victim
[2] Ver https://en.wikipedia.org/wiki/Berlin_Wall
[3] Ver https://es.wikipedia.org/wiki/Extrema_derecha
[4] Ver https://es.wikipedia.org/wiki/Estudio_de_la_Historia_(Arnold_J._Toynbee)

que su resultado más directo ha sido lanzar a Europa a indagar (como pollo sin cabeza) en todas las direcciones "de moda", a ver si pueden desarrollar capacidades de suficiente valor añadido como para justificar que el mundo siga contando con ella en las próximas décadas.

Aunque son varias las modas posibles, querría centrarme en solo dos. Por una parte, está el Problema esencial y todavía no resuelto, de los sistemas digitales actuales que es el de la **Identidad Digital**, y sus parientes cercanos que son la **Autenticación** y la **Autorización**. Por otra parte, está el pánico que se está intentando establecer sobre la inseguridad de los sistemas criptográficos actuales frente a la muy cacareada **Amenaza Cuántica**.

En el primer caso tenemos al Reglamento Europeo eIDAS2, y por otra, las recomendaciones de la Comisión Europea para desarrollar escenarios a prueba de ataques "cuánticos".

Segundas partes eIDAS

El 23 de julio de 2014 el Parlamento Europeo y el Consejo de la Unión Europea aprobaron la entrada en vigor del reglamento eIDAS (*electronic IDentification, Authentication and trust Services*), relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en Europa.

Además de definir los distintos tipos de firma electrónica, eIDAS regula también los servicios de: Sellado y marcado de tiempo, correo electrónico certificado, creación, verificación y validación de certificados para la autenticación de sitios web, documentos electrónicos, así como cuales deben ser los mecanismos de identificación y autenticación, sus distintos niveles y su interoperabilidad entre los estados miembros.

En 2021, aparece eIDAS2 que es la segunda versión del reglamento de Identificación Electrónica, Autenticación y Servicios de Confianza, cuyo objetivo es, una vez más, promover interacciones digitales seguras dentro y entre los estados miembros de la UE.

eIDAS proporciona cobertura legal para prestar servicios de confianza, implementar servicios de identificación, certificados digitales y firma electrónica, además de permitir la identificación remota por vídeo para aquellos casos en los que haga falta una verificación presencial de la identidad de las personas. Esencialmente, el eIDAS establecía un marco necesario para habilitar servicios de identificación y firma electrónica **reconocidos de forma mutua en los distintos estados miembros desde septiembre de 2018**.

Sin embargo, tan solo 14 países miembros han notificado al menos un sistema de identidad electrónica y **sólo un 59% de los residentes en la UE** tienen acceso a sistemas transfronterizos de identidad electrónica, lo que implica una escasa implantación en el sector público.

eIDAS2 es una nueva propuesta publicada el 3 de junio de 2021 que supone una evolución de eIDAS para atender las carencias identificadas, así como a su baja implantación en el sector público. eIDAS2 tienen como objetivo que de aquí al año 2030, su adopción llegue a un 80% de ciudadanos.

Sin embargo, eIDAS no cubre la provisión de **atributos electrónicos**, como certificados médicos o cualificaciones profesionales, dificultando el reconocimiento legal en Europa de estas credenciales. Además, tampoco permite el control por parte de los usuarios de los datos que se intercambian en los procesos de verificación.

Los eWallets no aportan ningún control duradero del titular a la distribución de sus datos. Una vez entregado el certificado de atributos, este documento digital auto-contenido, puede ser transmitido a terceros, acumulado en nuevas bases de datos, etc., y todo ello sin control real alguno por parte del titular. eIDAS tampoco permite el control por parte de los usuarios de los datos que se intercambian en los procesos de verificación.

Propuestas de eIDAS2

Por eso eIDAS2 propone la creación de una **identidad digital europea** "controlada" por los ciudadanos a través de una cartera o *wallet* de identidad digital (EDIW, **European Digital Identity Wallets**) y que pueda ser leída por cualquiera para verificar la identidad de los ciudadanos.

eIDAS2 amplía la lista de servicios de confianza incluyendo los **servicios de archivo electrónico**, los **libros mayores electrónicos**, la **gestión remota de dispositivos de firma electrónica** y la creación de **sellos electrónicos**.

Con eIDAS2 se facilitaría los procesos de verificación en cualquier circunstancia simplemente implantando la tecnología que lee el e-ID de los ciudadanos a través de sus eWallets. El uso de estos eWallets permitirá que sus titulares **se puedan identificar con su teléfono móvil** en **procesos *online* y presenciales** (*offline*) en su acceso a cualesquiera servicios.

Con la posesión y gestión de su eWallet, su titular podrá disponer de la información administrativa y datos de ciudadanos que estén en cualquier organismo público o privado, consultar expedientes, perfiles sanitarios, información fiscal, bancaria, universitaria, o de cualquier otro tipo. Así, por ejemplo, con su eWallet, el ciudadano podría abrir una cuenta bancaria en cualquier estado miembro de la UE, podría acceder a su perfil sanitario a través de la identidad digital europea, podría alquilar un vehículo o cualquier servicio mediante su e-ID, podría compartir datos financieros entre bancos de distintos estados miembros (ingresos, calificación crediticia, etc.).

La cartera de identidad digital de la UE

En eIDAS2 se define la **cartera de identidad digital de la unión europea** (IDUE) como: "*un producto y servicio que permite al usuario almacenar datos de identidad, credenciales y atributos vinculados a su identidad, con el fin de proporcionarlos a las partes informadas a petición de estas y de utilizarlos con fines de autenticación, en línea y fuera de línea, para un servicio de conformidad con lo dispuesto en el artículo 6 bis, así como para crear firmas y sellos electrónicos cualificados*".

En concreto el artículo 6.3 de la propuesta eIDAS 2 establece:

Las carteras de identidad digital europea permitirán al usuario:

a) solicitar y obtener, almacenar, seleccionar, combinar y compartir de forma segura, transparente y rastreable por el usuario, los datos de identificación de persona jurídica y la declaración electrónica de atributos que sean necesarios para autenticarse en línea y fuera de línea con el fin de acceder a servicios públicos y privados en línea;

b) firmar por medio de firmas electrónicas cualificadas.

Según esto, un ciudadano europeo podría llevar en el móvil y compartir de manera segura documentos como el DNI, el carnet de conducir, un título académico, la tarjeta sanitaria, recetas electrónicas, el carnet profesional, certificados bancarios, historiales médicos, entre otros.

La UE propone que cada estado miembro emita una cartera digital personal que permita a los ciudadanos almacenar y gestionar los datos de identidad y los **testimo-**

nios electrónicos de atributos de forma segura en sus dispositivos.

Un concepto clave en estos eWallets son los "atributos" que serían determinadas informaciones acerca de una persona. Por ejemplo, la fecha de nacimiento, las licencias profesionales o el expediente académico, credenciales societarias, etc. Estos atributos se autenticarán mediante una declaración electrónica certificada de atributos (testimonios), emitidas por cualquier entidad que tenga potestad para establecer lo testimoniado como una Universidad o un **Prestador Cualificado de Servicios de Testimonios** asociado a ella.

Con su eWallet el usuario podrá autenticarse e identificarse, almacenar e intercambiar informaciones administrativas como, por ejemplo, su nombre, apellidos, fecha de nacimiento, nacionalidad, derecho a residir, trabajar o estudiar en un determinado estado miembro, o incluso sus cualificaciones profesionales, historial de empleo o su solvencia crediticia.

Con este nuevo enfoque, la divulgación de los datos de identidad podría ser selectiva. Del mismo modo que las tarjetas bancarias se utilizan hoy en día para autorizar los pagos, las carteras digitales europeas **autorizarán la divulgación de información de confianza** sobre los usuarios a ciertas partes informadas, **bajo el efímero "control" del titular**.

Los usuarios de esas carteras llevarán en sus móviles una *app* que incorporará los datos electrónicos de identidad que ellos decidan y podrán utilizarlos en cualquier país de la Unión Europea. Una característica que también hay que tener en cuenta es que el eIDAS2 pretende incluir en el uso de ese eWallet la **gestión/autorización del usuario en el tratamiento de sus datos personales**. Se pretende que los usuarios puedan **limitar formalmente** la entrega de testimonios de atributos de identidad a los que sean estrictamente necesarios para recibir un servicio y, de algún modo, **que se pueda retirar el consentimiento para el tratamiento de datos**.

La idea es que el reglamento eIDAS2 se apruebe antes de las siguientes elecciones al Parlamento Europeo que están previstas para mayo/junio de 2024. Los estados miembros de la Unión Europea tendrían desde entonces, si no hay modificaciones sobre el texto inicial, menos de tres años para lanzar una cartera de identidad digital para sus ciudadanos.

El 1 de febrero de este año, la Comisión Europea hizo pública la primera "EU Toolbox[5] for the European Digital Identity Wallet (EUDI Wallet)", un proyecto clave desarrollado entre varios estados miembros. En línea con esta iniciativa, la Comisión también está desarrollando programas concretos en áreas de alta prioridad como son los carnets de conducir, los historiales médicos digitales, los pagos, y las cualificaciones profesionales.

Aunque todo este esfuerzo es encomiable dentro de la necesaria transformación de la Unión Europea en algo más que un mercado común de capitales, bienes y fuerza laboral, está por ver a dónde llega. Para empezar, ya estamos en la versión dos del eIDAS de hace ya bastantes años y una parte de su contenido es enmendar algunas ausencias de la versión inicial.

¿Y los análisis de seguridad de la propuesta?

Ahora bien, en la documentación europea consultada se echan en falta los análisis de seguridad de la propuesta. Por ejemplo, ¿qué pasa si un usuario pierde o le roban el móvil donde tiene instalado su eWallet electrónico? ¿Cuántas copias habrá de cada eWallet y dónde estarán guardadas, quién tendrá acceso a ellas?

Los eWallets que cada estado miembro desarrolle tendrán en común ser contenedores digitales, probablemente cifrados, que guarden en su interior los documentos públicos que constituyen los certificados digitales de atributos. El uso de esos contenedores, es decir, la extracción e inclusión de documentos en ellos, requerirán algún tipo de autenticación segura por parte del usuario (que sólo debería ser el titular) y ¿cómo se va a conseguir eso?

Los eWallets no son nada diferente a cualesquiera contenedores cifrados que ya hay en el escenario digital avanzado y, como ellos, tienen el mismo problema esencial: **la autenticación cierta y única del titular legítimo** de los mismos.

Otro frente que dejar en claro cuanto antes es que los eWallets no aportan ningún control duradero del titular a la distribución de sus datos. Una vez entregado el certificado de atributos, éste documento digital auto-contenido, puede ser transmitido a terceros, acumulado en nuevas bases de datos, etc., y todo ello sin control real alguno por parte del titular. Lo del consentimiento en la gestión de datos personales sigue siendo una norma sin posibilidad de exigir realmente su estricto cumplimiento. Los eWallets no tienen nada que ver con las quimeras de las Identidades Auto-Soberanas, aunque algunas veces puedan sonar parecidas.

Lo que sí hay que reconocerle a esta nueva **faltriquera digital** de la Unión Europea, es que podría/debería cambiar el modo de almacenar los datos de los ciudadanos y de los estados. Si cada uno de los titulares tuviera en exclusiva los documentos de atributos que le corresponden, **no existirían y podrían estar prohibidas las bases de datos centralizadas**. En ese caso, los ciudadanos podrían "desaparecer", voluntaria o involuntariamente, sin dejar el más mínino rastro y eso es malo, al menos para las necesidades historiográficas de cualquier sociedad avanzada.

Hay que reconocerle a esta nueva faltriquera digital de la UE que podría/debería cambiar el modo de almacenar los datos de los ciudadanos y de los estados. Si cada uno de los titulares tuviera en exclusiva los documentos de atributos que le corresponden, no existirían y podrían estar prohibidas las bases de datos centralizadas.

Por lo anterior, no es razonable pensar en que las únicas copias de los certificados de atributos fueran a estar en exclusiva en los eWallets de sus titulares; al menos existirán también, en bases de datos controladas por las fuentes que generan dichos atributos y con ello, una autoridad suficientemente elevada **podría reconstruir cualquier eWallet previamente generado** sin colaboración ni permiso de su titular.

En cualquier caso, la misma existencia de documentos digitales auto-contenidos, verificables por cualquiera, hace que, su uso, su presentación frente a quien así lo requiera, **suponga una inevitable fuga de información** y una posibilidad de reconstruir sin posible control grandes bases de datos sin el más mínimo consentimiento del titular.

Aunque las propuestas de los eWallets realmente hiciesen lo que prometen/insinúan, deberían estudiarse sus efectos en manos de una sociedad de **1) inadaptados tecnológicos** (por edad o por formación) y de **2) narcisistas despreocupados** del rastro digital que genera su frenética existencia en redes sociales y demás abrevaderos de moda; sobre todo porque, en conjunto, constituyen la mayoría de nuestras sociedades.

[5] Ver https://digital-strategy.ec.europa.eu/en/news/european-digital-identity-wallets-commission-publishes-first-technical-toolbox-towards-prototypes y https://ec.europa.eu/newsroom/dae/redirection/document/93678

Amenaza Cuántica

Todos los documentos y noticias relacionadas con la computación cuántica y su impacto sobre los sistemas de seguridad actuales deben analizarse con cuidado, no vaya a ser que seamos víctimas de algún engaño. En todos los casos que me vienen a la memoria[7], todos los discursos parten de axiomas que aceptan, **como acto de fe y sin el más mínimo rubor**, que la Computación Cuántica ya está aquí y que en cuestión de pocos años que los actuales Criptosistemas Asimétricos dejaran inexorablemente de ser aceptablemente seguros.

A la luz de esa "*verdad revelada*" (¿por quién, a quién y en beneficio efectivo de quién?) se lanzan **1)** campañas de renovación de los **criptosistemas asimétricos** con **algoritmos completamente nuevos, inmaduros** y **no suficientemente probados**, y **2)** la inminencia de la amenaza diciendo que "*los malos*" (¿quiénes serán realmente? ¿qué pruebas hay de ello?) ya están guardando información cifrada "*para poderla descifrar cuando tengan disponibles ordenadores cuánticos*" como quien tiene PCs, tabletas o GPUs a su capricho.

Estos razonamientos, me recuerdan al **Melanocetus johnsonii**[8] (Diablo Negro), pez abisal que muestra a la víctima una lucecita (bioluminiscencia) que aterroriza o atrae al pececillo y le invita a huir en la dirección contraria que es, precisamente, donde le espera el depredador con su enorme boca seguida de sus sistema digestivo.

En nuestro escenario no creo que en la dirección marcada por la Amenaza Cuántica esté ningún depredador dispuesto a digerirnos, pero sí veo **legiones de pescadores que se benefician de aguas tan revueltas**. Al final, ya no es que los centenares de millones que gasta la Unión Europea en estos temas terminen siendo simplemente "*beneficio de pescadores*" (no necesariamente europeos, ni generadores de ninguna tecnología revolucionaria), sino que esas **pérdidas evitables 1)** nos lastran en lo de encontrar de un puesto avanzado para Europa en la geopolítica del futuro planeta y, evidentemente, **2) no resuelven el problema de que las tecnologías de seguridad actuales no son eternamente infalibles** y requieren de un natural y continuo mantenimiento como cualquier otro ejemplo del ingenio humano.

Hoy en día no pueden considerarse seguras longitudes de claves que sí lo eran hace 30 años, ni las actuales longitudes de claves pueden considerarse eternamente seguras, por lo que el miedo a que dentro de cierto tiempo sí tendrán tus enemigos capacidad para entender lo que ahora cifras, **es algo que siempre ha estado ahí** y que no es patrimonio de ninguna Amenaza Cuántica.

Recordemos que ya en 1949 el irrepetible Claude Shannon[9] demostró[10] que los algoritmos conocidos hasta entonces eran "*rompibles*" todos, excepto uno. Ese autor nunca publicó –porque no lo sabía– cómo podían romperse efectivamente, pero sí estableció, sin lugar a dudas, que algún día podrían romperse. A pesar de haber reducido el arsenal criptográfico a un solo algoritmo seguro, el cifrado de Vernam[11] u OTP[12], el mundo siguió adelante adaptando las seguridades efectivas de los distintos algoritmos a las capacidades de sus contrincantes y teniendo en cuenta la variable tiempo; lo que hoy es imposible, mañana podrá ser difícil, pero acabaremos viendo que es muy fácil.

Si llegan los ordenadores cuánticos algún día, veremos **1)** si realmente son una amenaza, y **2)** alargaremos las longitudes de las claves para que sean inservibles (los Quantum Computers) durante cierto tiempo. El secreto eterno existe, pero no de la manera que algunos piensan. **El secreto eterno existe siempre que sea irreversible**.

No hay ningún proceso documentado cuyo secreto pueda considerarse eterno mientras existan los contenidos de esos documentos o registros (incluso si en su momento fueron cifrados). La única posibilidad de que algo permanezca en secreto eternamente es que no quede de ese algo nada escrito, ningún registro, ningún testigo, ningún recuerdo. En la historia de la humanidad hay innumerables hechos que permanecen secretos y que siempre lo estarán, y todos ellos tienen en común que de ellos no hay el mas mínimo registro, documento, o testigo.

La Amenaza Cuántica no resulta ser una amenaza tan amenazante como algunos están interesados en hacernos creer, y dedicarle excesiva atención (peor aún si es en exclusiva) **no va a ayudar a Europa en su búsqueda de un lugar bajo el futuro sol**. Sin embargo, sí le puede hacer perder un montón de recursos, tiempo y oportunidades alternativas no identificadas.

Conclusiones

La psicología de las sociedades no es muy diferente de la de sus individuos, por lo que en las decisiones gubernamentales (nacionales o supranacionales) no es raro ver componentes fácilmente identificables en el comportamiento de cualquiera. Por ello, es razonable esperar que también haya modas en el comportamiento de los estados. Lo que no es tan fácil de aceptar es que, además, no haya una componente racional en lo que estos entes supra-ciudadanos hacen o persiguen. Lo que pasa es que la racionalidad no es única, sino que depende del modelo lógico en el que se basa, por lo que es razonable en uno puede no serlo en otro.

El secreto eterno existe siempre que sea irreversible. No hay ningún proceso documentado cuyo secreto pueda considerarse eterno mientras existan los contenidos de esos documentos o registros (incluso si en su momento fueron cifrados).

Teniendo en cuenta que estamos viviendo en el modelo lógico del máximo beneficio para el capital, muy bien pueden tener éxito medidas tomadas a la sombra de modas[13] caprichosas y sin justificación objetiva comprobable pero, aun así, no por ello van a ser una estrategia inteligente pensando en el medio o largo plazo.

En nuestra realidad sigue pendiente **el problema de la autenticación robusta y segura** de individuos físicos y jurídicos y los eWallet no van a arreglar este problema, pero sí van a abrir la posibilidad de que los europeos nos involucremos algo más en la custodia y circulación de nuestros datos personales, ¡Algo es algo y con ello *Europe would be different*!

Lo que sí está claro es que el tinglado de la Europa actual no está como para poder caer en despilfarros tan engorrosos como los asociados con nuevas versiones cuánticas del tradicional cuento de "Pedro y el lobo", y no terminar pagándolo con futuras irrelevancias a medio y largo plazo. ■

[6] Ver https://dle.rae.es/faltriquera
[7] Ver, por ejemplo, https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf
[8] Ver https://en.wikipedia.org/wiki/Humpback_anglerfish
[9] Ver https://en.wikipedia.org/wiki/Claude_Shannon
[10] Ver https://en.wikipedia.org/wiki/Communication_Theory_of_Secrecy_Systems
[11] Ver https://en.wikipedia.org/wiki/Gilbert_Vernam
[12] Ver https://en.wikipedia.org/wiki/One-time_pad
[13] Ver https://dle.rae.es/moda

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es