>> Jorge Dávila

El Canto de la Sibila[1] en la Ciberseguridad de 2024

Es fácil entender que cuando uno es atacado debe escapar y, si es necesario, defenderse; además no tiene otra opción si quiere sobrevivir, sin embargo, la defensa no siempre es la estrategia más inteligente. Siempre hay la posibilidad de evitar el riesgo, 1) impidiendo que el ataque se produzca (si eso fuese de alguna manera posible), o 2) impidiendo que el ataque tenga efecto. La digitalización de la sociedad cambia muchas cosas y, con ellas, incluye debilidades que deberíamos tener presentes y en cuenta ANTES de sumergirnos irreversiblemente en ella. Empecemos el año jugando a profetas de desastres, ya que la Ley de Murphy[2] siempre estará de nuestro lado…

A pesar del disgusto de la Iglesia Católica, todavía se celebra en las Misas del Gallo de algunas catedrales mediterráneas el drama litúrgico de melodía gregoriana conocido como **el Canto de la Sibila**[3] (*Cant de la Sibil·la*). Esta liturgia es una tradición que se viene realizando desde la Baja Edad Media[4] y que perdura hasta nuestros días. Incluso sobrevivió a su prohibición expresa en el **Concilio de Trento** (1545–1563) y el 16 de noviembre de 2010 fue declarado por la UNESCO **Patrimonio Inmaterial de la Humanidad**.

La sibila es interpretada por una mujer o un niño vestido de mujer, y actúa como la **profetisa del fin del mundo**[5] de la mitología clásica pero adaptada al cristianismo gracias al gusto de este último con el **juicio final** y el final de los tiempos.

En este contexto, la Revista SIC en su primer número de cada año, gusta de consultar a un considerable número de agentes de la Ciberseguridad patria y que aquí operan, así como a una nutrida representación de actores y agentes internacionales concernidos, pidiéndoles que vaticinen los peligros, desastres, tecnologías, modelos de negocio maligno, etc., que pueden darse en el año que empieza. Es una especie de consulta a la Sibila colectiva de la ciberseguridad que, como aquella, suele acertar menos que una escopeta de feria (algo típico de las predicciones, las haga éstas quien las haga).

Con el ánimo de minimizar los fallos, y desde el año pasado, la Revista no pide a sus Sibilas atinar con lo que realmente va a materializarse en el año en curso, y ahora sólo les solicita "*Amenazas y ciberataques en 2024: ¿cuáles serán los más complejos y de gran impacto, se esperen o no?*". Esta ampliación de horizonte es de agradecer para no poner de manifiesto que **1)** con toda probabilidad **va a seguir pasando lo que ya pasaba el año anterior**, y **2)** realmente **no tenemos mucha idea** de qué puede terminar pasando en 2024.

Puestos en esta tesitura, lo que sí podemos hacer es echar un vistazo calmado a **1)** lo que se ha terminado convirtiendo la digitalización de nuestra sociedad actual, y **2)** esa nueva "industria" que es el dueto Ciberseguridad-Ciberdelincuencia.

Dado que la evolución de cualquier sociedad es lenta en la escala temporal de generaciones de ciudadanos, lo es más aún si se trata de la sociedad en su totalidad y estamos hablando del "primer mundo" a nivel planetario.

En nuestras sociedades es más importante la firma digital de los contratos de todo tipo que el secreto de esas mismas transacciones o contratos. El trazado, autenticación e identificación de las transacciones tiene efectos colaterales muy significativos, estratégicos y que, sin duda alguna, serán peligrosos para alguien. ¿Para quién?

Lo más probable es que este año ocurra lo mismo que ocurría el año pasado: **1) consolidación e industrialización de la ciberdelincuencia**, **2)** los **problemas de autenticación** seguirán como estaban (sin resolver), **3) la indiscutible atribución de cualquier cosa en la red será imposible** a menos que el ataque/acción se haga muy muy mal. **4)** La **Identidad digital segura estará ausente** y no se la esperará, **5)** seguiremos utilizando los **mismos instrumentos de identificación y firma digital** (*tokens* software de la FNMT, 2FAs, pares usuario-contraseña o similares) para que mínimamente funcione el tinglado digital de las distintas administraciones (tanto públicas como comerciales). **6)** Los **documentos nacionales de identidad digital** (eIDAS), europeos o patrios (eDNI), **seguirán intentando hacerse un sitio bajo el sol**, y **7)** el Libre Mercado de la EU avanzará en el proceso de arrebatar a los Ministerios del Interior de los estados miembro la exclusiva de ser ellos los que emitan, en última instancia, la identidad digital (**EU Wallet**[6]) de los ciudadanos humanos y analógicos, ya que, por otra parte, **8)** la **identidad digital de entidades jurídicas** (empresas y demás constructos legales) y de **lo que no son ciudadanos** (**IoT** & **OT**) claramente llegará, cuando llegue, de iniciativas no gubernamentales. **9) El negocio de la Ciberseguridad** seguirá siendo cada día **más productivo en lo que a los beneficios económicos** se refiere, pero **no mejorará su tasa de éxito frente a sus contrincantes** naturales que son los ciber delincuentes, las agencias de inteligencia, las Policías y las Fuerzas Armadas. **10)** En este año, la **digitalización de todos los aspectos de la sociedad continuará**, incluso a una velocidad superior que en años anteriores, con lo que paralelamente **11)** seguirá aumentando las posibilidades de **la cibervigilancia y del capitalismo que lleva subyacente** (*IA trainers*, "científicos de datos", ESO y Marketing Dirigido, *influencers* y manipulación informativa, frecuentes campañas de *fake news*, erosión de la confianza social y, consecuentemente, la erosión del Contrato Social[7] roussoniano, etc.).

Sin embargo, también podemos intentar, como el Apóstol San Juan[8], o como el Beato de Liebana[9] en su "**Comentario al Apocalipsis**"[10], imaginar cómo será ese capítulo final –siempre por llegar–, y escribir un nuevo "Libro de las Revelaciones"[11] con el que "*regalar miedo a la población y así para poder venderles más (ciber)seguridad*".

En este sentido, y para no repetirnos, hay

que revisar aspectos diferentes a los ya estudiados durante años anteriores. Desde que la información en poder, es decir, desde que la Sociedad es Sociedad [12], la protección de la confidencialidad (secreto) ha sido una obsesión continua de los poderosos (que querían seguir siéndolo). Desde el mismo momento que se inventa la escritura, también se inventan los métodos criptográficos [13] y durante siglos eso ha sido lo que ha preocupado y contentado a Papas, Reyes, Gobernadores y Militares.

El problema es que a pesar de estar plagado de problemas potenciales y algunos muy reales como el de la carencia de credenciales de identidad no hackeables, la sociedad sigue digitalizándose cada vez más y pronto todo el tejido social será digital.

Sin embargo, la digitalización de la sociedad va más allá del mismo poder sobre ella. La digitalización de la sociedad afecta y se dirige al mismo funcionamiento de la misma. En nuestras sociedades **es más importante la firma digital** de los contratos de todo tipo **que el secreto** de esas mismas transacciones o contratos. De hecho, actualmente hay fuerzas que quieren llevarnos [14] a "sociedades transparentes" [15] (esperemos que sean reciprocas), en concreto en lo que al dinero en efectivo se refiere, y en las que no haya secreto, pero aun así siempre será necesario que sean **autenticables** (pero no necesariamente **identificables**). En cualquier caso, para que se dé una transacción siempre tiene que estar claro lo transferido, la cuantía pagada, la moneda utilizada y de qué cuenta sale el dinero y a cuál va a parar. Otra cosa distinta es la identificación de los participantes, con la que esa operación se pueda relacionar con otra identidad ajena al mundillo digital, como puede ser la identidad de las personas físicas/jurídicas involucradas y que tiene derechos y responsabilidades legales.

Algunos países propugnan el abandono del papel moneda para hacer completamente trazables todas las transacciones económicas [16] pero mucho me temo que esa transparencia se quede para la inmensa mayoría de ciudadanos (no ricos). Y que siempre quede un paraíso financiero muy exclusivo, una zona ciega en la que los ricos puedan mover sus riquezas sin ser observados por esos insaciables recaudadores de impuestos que quieren hacerles partícipes de la construcción de lo público, de lo de todos y para todos.

En cualquier caso, ese tipo de incitativas hay que analizarlas con mucho cuidado antes de ponerlas en marcha ya que **el trazado, autenticación e identificación de las transacciones tiene efectos colaterales muy significativos,**

Erradicar las Mafias siempre ha sido muy difícil, sobre todo cuando con anterioridad fueron compañeras toleradas de viaje (la Cosa Nostra en la liberación de Italia del fascismo, apoyo a los Talibanes en la Guerras Civil y Ruso-Afgana por parte de la CIA, la Contra Nicaragüense en tiempos de Carter, etc.) pero, en cualquier caso, lo único eficaz para acabar con ellas es la asfixia económica y la desmovilización espontánea de sus bases.

estratégicos y que, sin duda alguna, serán **peligrosos para alguien**. ¿Para quién? Antes de hacer grandes cambios hay que elegir, de forma consciente e informada, para quién el cambio debe/puede suponer un riesgo.

Además de todo esto, **la digitalización también aporta grandes ventajas a las sociedades que la acogen en su seno**. La velocidad de comunicación, la distancia a las que puede darse, el volumen y naturaleza de lo compartido no tiene parangón con tecnologías antes conocidas por el hombre. Los **registros** de todo tipo que constituyen el tejido administrativo esencial de cualquier sociedad, en su liberación del papel y la tinta han saltado a unas dimensiones en las que el tamaño, detalle y velocidad de acceso e inmediatez, prácticamente no tienen límite; como no lo tiene el tamaño de la sociedad que se podría gestionar [17] gracias a la digitalización y a la deslocalización geográfica que aportan las redes.

Para que esos registros digitales desempeñen sus funciones es necesario resolver antes el problema de la **Identidad Digital**, y este es un **problema antiguo todavía pendiente de solución**. Con más de treinta y cinco años a su espaldas [18], todavía no nos hemos dotado de un sistema de identificación digital adecuado técnica y socialmente. Técnicamente tenemos el problema de **1)** vincular **de forma indisoluble** la identidad digital y la voluntad (libre e informada) de su titular, de **2)** hacer que ésta, la identidad digital y el dispositivo que la custodie y ejerza **sean únicos e irrepetibles**, y de **3)** hacer que sea tan sencilla y agradable de utilizar que su difusión y asunción sea espontánea a todos los niveles y por todos los miembros de la sociedad a la que sirve. Cualquier propuesta compleja, oscura, y que excluya de un plumazo sectores enteros de sus necesarios usuarios (eDNI) esta abocada al fracaso económico y a un alto coste de oportunidad [19].

Las soluciones europeas eIDAS [20] y sus faltriqueras [21] digitales (EUDI Wallet [22]) están bien como **idea seminal** que establezca definitivamente la necesidad de **1)** una **identificación transfronteriza ágil y sencilla** de personas físicas y jurídicas, así como de servicios prestados, que sea aceptada en toda Europa, y **2)** que **unifique e incentive** las iniciativas que puedan existir en los distintos estados nacionales europeos. Sin embargo, sigue sin satisfacer las necesidades técnicas antes mencionadas. Mientras se siga viendo

[1] Ver https://en.wikipedia.org/wiki/Sibyl y https://en.wikipedia.org/wiki/Cumaean_Sibyl
[2] Ver https://en.wikipedia.org/wiki/Murphy's_law
[3] Ver https://es.wikipedia.org/wiki/Canto_de_la_Sibila
[4] En España el documento más antiguo que se conserva es un manuscrito visigodo de la mezquita de Córdoba del año 960 y perteneciente a la liturgia mozárabe; es decir, de la población cristiana de origen hispanovisigodo, que vivía en el territorio de Al-Ándalus y que, como los judíos, eran "dhimmis" ("gentes del Libro"; es decir, monoteístas de religiones Abrahámicas que estaban protegidos por el Islam)
[5] Ver https://historia.nationalgeographic.com.es/a/profecia-fin-mundo-creencia-colectiva_19971
[6] Ver https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/
[7] Ver https://en.wikipedia.org/wiki/The_Social_Contract
[8] Ver https://en.wikipedia.org/wiki/John_the_Apostle
[9] Ver https://en.wikipedia.org/wiki/Beatus_of_Liébana
[10] Ver https://en.wikipedia.org/wiki/Commentary_on_the_Apocalypse
[11] Ver https://en.wikipedia.org/wiki/Book_of_Revelation
[12] Ver https://en.wikipedia.org/wiki/Hammurabi
[13] Método criptográfico = Alteración reversible e intencionada (por parte de los comunicantes) de las reglas de codificación (escritura) del mensaje.
[14] Ver https://blog.caixabank.es/blogcaixabank/paises-sin-efectivo/#
[15] Ver Vattimo Gianni La Sociedad Transparente by Gianni Vattimo
[16] "The Heretic's Guide to Global Finance: Hacking the Future of Money" by Brett Scott (Ver https://es.wikipedia.org/wiki/Brett_Scott)
[17] Ver https://en.wikipedia.org/wiki/World_population
[18] Ver https://en.wikipedia.org/wiki/X.509
[19] Ver https://en.wikipedia.org/wiki/Opportunity_cost
[20] Ver https://en.wikipedia.org/wiki/EIDAS
[21] Ver https://es.wikipedia.org/wiki/Faltriquera
[22] Ver https://eudiwalletconsortium.org/

el problema de la identidad digital como una oportunidad mercantil y económica de vender documentos nacionales de identidad digitales, el problema no se resolverá, y seguiremos agrandando el panteón de carísimas intentonas que en tres décadas solo han dejado **cosas que pudieron ser y no han sido**.

El problema es que, a pesar de todo esto, a pesar de estar plagado de problemas potenciales y algunos muy reales como el de la carencia de **credenciales de identidad no hackeables**, la sociedad sigue digitalizándose cada vez más y pronto todo el tejido social será digital. Nos estamos entregando al sueño interesado de algunos sin pensar que podamos estar, con ese mismo hecho, escribiendo la inviabilidad anunciada de esa sociedad recién nacida.

Posibles desastres digitales

Puestos a pensar en posibles desastres digitales y aprendiendo del nunca bien ponderado ejemplo del *ransomware*, podemos encontrar profecías apocalípticas que den lustre a los cantos de Sibila que se nos piden. El problema de las sociedades es que **1) su organización interna determina el éxito** histórico (duración) y el tamaño de las mismas, y **2)** su **fuerza de cohesión** puede nacer **del miedo, la coacción y/o de las creencias**, fundadas o no, experimentables o fantásticas, de su población pero, en cualquier caso, **se basan en la confianza** que los individuos y conjuntos de individuos depositan (¿ciegamente?) en el líder o en el estado.

Erradicar las Mafias siempre ha sido muy difícil, sobre todo cuando con anterioridad han sido compañeras toleradas de viaje (la **Cosa Nostra**[23] en la liberación de Italia del fascismo, apoyo a los **Talibanes**[24] en la Guerras Civil y Ruso-Afgana[25] por parte de la CIA, la **Contra** nicaragüense en tiempos de Jimmy Carter[26], etc.) pero, en cualquier caso, lo único eficaz para acabar con ellas es **1)** la **asfixia económica** y **2)** la **desmovilización espontánea** de sus bases[27].

Un mecanismo muy eficiente en la desmovilización generalizada de las bases es **la pérdida de confianza en el sistema, y la sensación de no haber futuro**. Una sociedad confía en la corrección de todos los datos que utiliza para su funcionamiento y en todos los que ha generado durante los años anteriores de existencia. **Toda sociedad cimenta su confianza en ella misma en la integridad de los registros que la constituyen**. Alterar la integridad de registro basados en documentos de papel[28] ha sido el negocio de falsificadores de todos los tipos y en todas las circunstancias[29].

Aun siendo difícil, la autenticación de tintas, papeles, grafías y demás elementos de los registros analógicos, se puede hacer[30] y todos los falsificadores clásicos (analógicos) tarde o temprano han sido descubiertos, tanto ellos como sus obras. Sin embargo, en el escenario digital, el original es esencialmente idéntico a sus copias, por lo que la "falsificación" (copia) es indetectable como tal; es indistinguible del original. Lo mismo ocurre con dos versiones ligeramente distintas de un objeto digital ¿Cuál es la verdadera? Sin medidas operativas y criptográficas[31] correctamente implementadas y utilizadas[32], es imposible establecer la integridad[33] (capacidad de no haber sido alterada) de ningún objeto digital.

En el escenario digital, el original es esencialmente idéntico a sus copias, por lo que la "falsificación" es indetectable como tal e indistinguible del original. Lo mismo ocurre con dos versiones ligeramente distintas de un objeto digital ¿Cuál es la verdadera? Sin medidas operativas y criptográficas correctamente implementadas y utilizadas, es imposible establecer la integridad de ningún objeto digital.

La contaminación de las bases de datos

Si todos los elementos de las sociedades digitales (ciudadanos, empresas, administración, el capital, la justicia, etc.) construyen y fundamentan su confianza en la integridad de sus registros y de sus bases de datos, **qué pasaría si** alguien lograse y demostrase (públicamente) haber sido capaz de alterar la integridad referencial[34] y/o de entidades[35] en alguna bases de datos relacionales útiles en nuestro día a día, o en nuestra historia (registro civil, catastro, banca y sistema financiero, sistema de salud, etc.). Esa contaminación de las bases de datos podría minar la confianza de la sociedad en sus registros. Está claro que los **ataques por envenenamiento de bases de datos** habría que hacerlos de tal manera que desactivasen la política de copias de seguridad que se esté utilizando, pero eso es relativamente posible **si los ataques se hacen de forma discreta, minoritaria y prolongados en el tiempo**.

¿Cuánto pagaría el afectado por recuperar la integridad de su base de datos obteniendo del atacante la relación de cosas que ha cambiado? ¿Cuánto pagaría el atacado por que todo el mundo no supiera que sus bases de datos ya no son íntegras y no hay modo de recuperarlas? Hay varios otros escenarios (potencialmente apocalípticos) relacionados con la posible falta de integridad de las bases de datos en Sanidad y en Banca y Sistemas Financieros, pero no hace falta ser mucho más prolijos para hacer entender el mensaje. El *ransomware*[36] nos ha demostrado desde agosto de 2005[37] que es un modelo de ataque extremadamente sencillo y productivo[38] para el que ataca.

Tal y como se hacen las cosas hasta la fecha, no solo no sabemos si el gato de Schrödinger[39] está vivo o muerto. Tampoco sabemos **quién nos ha tocado las Bases de Datos** en la que confiamos ciegamente y las que rigen nuestra existencia, queramos o no. Nosotros no lo sabemos, pero los responsables de saberlo… tampoco. ■

[23] Ver https://en.wikipedia.org/wiki/Sicilian_Mafia
[24] Ver https://en.wikipedia.org/wiki/Operation_Cyclone
[25] Ver https://en.wikipedia.org/wiki/Soviet-Afghan_War y https://en.wikipedia.org/wiki/Afghan_Civil_War_(1992-1996)
[26] Ver https://en.wikipedia.org/wiki/Contras y https://en.wikipedia.org/wiki/CIA_activities_in_Nicaragua
[27] Ver https://en.wikipedia.org/wiki/Revolutions_of_1989
[28] Ver https://es.wikipedia.org/wiki/Lucio_Urtubia
[29] Ver https://news.un.org/es/story/2022/05/1508022
[30] Ver https://www.interpol.int/es/Delitos/Falsificacion-de-moneda-y-documentos-de-seguridad/Falsificacion-de-moneda
[31] Ver https://en.wikipedia.org/wiki/Message_authentication
[32] Ver https://en.wikipedia.org/wiki/Data_integrity
[33] La integridad se refiere a la calidad de íntegro, el estado de lo que está completo o tiene todas sus partes, es la totalidad, la plenitud. Integridad deriva también del adjetivo integer (in-, que significa no, y la raíz del verbo *tangere*, que significa tocar o alcanzar). Significa intacto, entero, no tocado o no alcanzado por un mal.
[34] Ver https://en.wikipedia.org/wiki/Referential_integrity
[35] Ver https://en.wikipedia.org/wiki/Entity_integrity
[36] Ver https://en.wikipedia.org/wiki/Ransomware
[37] Ver, por ejemplo, https://en.wikipedia.org/wiki/PGPCoder
[38] Ver https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/
[39] Ver https://en.wikipedia.org/wiki/Schrödinger's_cat

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