COMPLIANCE 360

Programa formativo en materia de compliance para entidades del tercer sector

BLOQUE 9

COMPLIANCE, DIGITALIZACIÓN Y NUEVAS TECNOLOGÍAS

Sesión 14 (11 de diciembre de 2024): **Cómo aplicar las nuevas tecnologías a nuestro sistema de compliance**

Sesión impartida por: C. Yvonne Mähler Lucini y por Ariadna Holguín Jimeno (Centro de Estudios Garrigues)

1. Compliance tecnológico

El compliance tecnológico es una rama dentro del compliance. Se encarga de evaluar y determinar los riesgos legales del uso de las Nuevas Tecnologías.

Debe tenerse encuentra dentro del programa de compliance de toda entidad, diferenciando dos vertientes:

- Compliance para el compliance: el control en el uso de herramientas que garantizan el cumplimiento del compliance es en sí mismo un riesgo que debe ser analizado por el *compliance officer*, pues no todas las herramientas tecnológicas cumplirán igual con la normativa.
- Compliance para la digitalización: evaluación y determinación de conflictos jurídicos que se suceden en el uso de las tecnologías en el funcionamiento diario de los organismo o entidades.

En ambos casos, deberemos realizar un estudio de las aplicaciones que se van a utilizar, analizar si esas soluciones software están adaptadas a la normativa y si efectivamente

son fiables, pues aunque la responsabilidad de una brecha de seguridad o de una ataque cibernético por fallas por ejemplo en el código pueden ser responsabilidad de la empresa que pone a disposición del software, el usuario debe tener un protocolo de actuación para estas situaciones y el riesgo asumido no será igual si existe evaluación del impacto de esa tecnología.

Se deberá añadir al mapa de riesgos comunes los tecnológicos, teniendo en cuenta normativas de privacidad, derechos digitales, consumidores y usuarios, medios de pago, plataformas de intermediación, uso de la inteligencia artificial, propiedad intelectual e industrial, entre otras.

Como todo sistema de compliance, deberá elaborarse en un protocolo de seguridad adaptado a las necesidades de la entidad, definiendo con claridad el uso de las tecnologías, sus límites y las fórmulas para garantizar y mantener la seguridad de la información y las comunicaciones. Definición de responsabilidades, clasificación de la información, delimitación de accesos o controles y medidas para las incidencias, serán ejes centrales en la ejecución del sistema de compliance tecnológico.

Garantizando el acceso a la información y a la formación a todos los miembros de la organización, pues serán éstos los que nos garanticen el menor impacto de incumplimiento.

2. Introducción a las Nuevas Tecnologías

Las Nuevas Tecnologías son un conjunto de tecnologías disruptivas que, englobadas dentro de la 4ª Revolución Industrial, están marcando un cambio de modelo productivo, industrial y social de las economías globalizadas.

a) Blockchain.

Qué es, cómo funciona y usos

El art. 3.1 subapartados 1 y 2 del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) nº 1093/2010 y (UE) nº 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 (en adelante, la Reglamento «MiCA») en relación con la

«Tecnología de registro descentralizado» o «TRD» la define como un tipo de tecnología que soporta el registro descentralizado de datos cifrados.

Será aplicable a partir del 30 de diciembre de 2024.

30.06.2024 será de aplicación: títulos referidos a las fichas referenciadas a activos y fichas de dinero electrónico

La tecnología Blockchain o de cadena de bloques es una tipología de las DLT (tecnología de registro distribuido) que concatena bloques en orden cronológico, vinculados entre sí y protegidos por pruebas criptográficas.

Esta tecnología supone una elección de los usuarios y desarrolladores lo que denominamos el Trilema técnico de la Blockchain:

Descentralización: no existe un control central sobre la estructura, se descentraliza en cada usuario o nodo. Todos los nodos tienen acceso a los mismos datos ya que la cadena de bloques permite que la creación de nuevos bloques se realice con la información contenida de todos los anteriores. La información se valida mediante el protocolo de consenso. Esta descentralización dará lugar a la Web 3 (actualmente utilizamos la web 2), en la que el usuario tendrá control absoluto sobre sus datos y su vida en línea, una definición que asumimos sencilla de web 3 la esbozó Packy McCormick: "una internet que es propiedad de los desarrolladores y los usuarios, coordinada con tokens"

Seguridad: es una de las cuestiones que genera más conflicto en esta materia, pues la descentralización fomenta ataques indeseados. Esta solución se encontrará a través de los protocolos de consenso y sus sistemas criptográficos. Además, la replicabilidad del contenido de los bloques garantiza que la información contenida en ellos siempre será la validada por los usuarios.

Escalabilidad: hace referencia al crecimiento exponencial de la estructura y aceptar cada vez más transacciones.

Hay que tener en cuenta que cuando se busca optimizar una de las tres propiedades otra se verá debilitada. Hay muchas fórmulas para resolver este trilema.

Actualmente, y tras el *merge* (transición de un protocolo de consenso "proof of work" a un protocolo de consenso "proof of stake") de Ethereum y la regulación de los ETF de Bitcoin (fondos cotizados en bolsa referenciados a Bitcoin) y Ethereum en EEUU así como nuestra andadura europea a través de MiCA, han supuesto un nuevo trilema, que según Paul Brody de EY, se refiere a productos, clientes y aprobación regulatoria.

Tipologías de Blockchain:

- Pública: cualquier persona puede unirse libremente a la red sin permisos, pudiendo ver, participar y validar transacciones. Principales redes públicas: Ethereum y Bitcoin. Aquí se priman la trasparencia y descentralización. Los participantes de la red se denominan mineros, ya que son los que minan los bloques a cambio del token o criptomoneda. El código es *open source* o abierto
- Privada: el acceso se limita y restringe, por lo que los participantes suelen estar autorizados previamente. Esta fórmula prima la seguridad frente a la descentralización y la transparencia. Son interesantes para organizaciones, sociedades o negocios que quieran limitar los accesos a su registro.
- Permisionada: El acceso está constituido por un sistema de permisos y controlado por una unidad central, el acceso al libro de transacciones es privado y no suele tener sistema de recompensas. Ejemplo: Hyperledger.
- Híbrida: es una red que une características de las dos primeras. La participación será privada mientras que el registro transaccional será público y verificable. No hay sistema de recompensas o minería. Puede ser una tipología utilizada por gobiernos u organizaciones que quieran compartir información segura, transparente y confiable.

¿Qué es un protocolo de consenso?

Es la fórmula por la que los miembros de la blockchain están de acuerdo para validar las transacciones que formarán los bloques de la cadena. Tipos:

- Proof of work (PoW): bitcoin
- Proof of stake (PoS): Ethereum
- Proof of importance (PoI)
- Ouroboros

- Proof of burn (PoB)
- Proof of capacity (PoC)
- Proof of authority
- Protocolo de consenso QBFT: Quorum Byzantine Fault Tolerance: se utilizan preeminentemente en blockchains privadas y de corte empresarial, buscando confiabilidad y eficiencia. La idea principal es la operatividad del "principio de tolerancia a fallas bizantinas" que busca un funcionamiento constante de la red de forma confiable incluso existiendo nodos maliciosos o que fallen. Otras que se desarrollen

La aplicación práctica de la tecnología Blockchain en el sector de las entidades sin ánimo de lucro.

- Auditoria
- Contabilidad
- Ciberseguridad
- Banca y pagos
- Seguros
- Supply chain
- Predicciones
- Alquileres
- Financiación
- Política
- Educación
- Energía
- Venta
- Inmobiliario
- Sanidad
- Caridad
- Iniciativas humanitarias

Algunos usos interesantes para las entidades del Tercer Sector:

Donaciones, financiación, transparencia y rendición de cuentas: beneficia la transparencia y la trazabilidad en la gestión de los activos. Podrían utilizar esta tecnología para proporcionar un registro inmutable y transparente para las transacciones de contenido económico, garantizando el propósito previsto para cada activo, de conformidad con los objetivos.

Ejemplos prácticos:

- Rastreo del café desde el momento en que se recogen los granos: trazabilidad para garantizar una obtención del producto responsable y sostenible
- Conversión de residuos plásticos en valor monetario
- Extracción minera sostenible y responsable
- Asistencia ante desastre naturales

Normativas que deben ser tenidas en cuenta

Protección de datos de carácter personal: RGPD y LOPDGDD, así como las resoluciones de las Autoridades nacionales y europeas que en esta materia vienen a dar forma a cuestiones que aún están faltas de regulación.

¿La Evaluación de Impacto?

Art. 35 RGPD: "Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares."

Encriptación de la información almacenada en los nodos: determinar si es anonimizada o seudonimizada. Método de encriptado: hashing → se trata de una técnica de seudonimización y por tanto está sujeta a la aplicación del RGPD.

Es por ello, y junto con otras resoluciones de la propia Autoridad de Control española junto con otras de ámbito europeo, los datos contenidos en la BC están sujetos a RGPD si no se utilizan otros medios para conseguir la anonimización.

Derechos de autor, propiedad intelectual e industrial. Las bases de datos.

Reguladas en el Titulo VIII del Libro II de la LPI arts. 133-137.

Se transpone la Directiva 96/9/CE a derecho español por medio de la Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

El derecho «*sui generis*» sobre una base de datos protege la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza su fabricante ya sea de medios financieros, empleo de tiempo, esfuerzo, energía u otros de similar naturaleza, para la obtención, verificación o presentación de su contenido.

Se protege el contenido económico de estas creaciones: se busca evitar que terceros exploten económicamente esas bases de datos. Debe existir una inversión sustancial, y puede ser inversión financiera, temporal, medial, energética, o similar.

Si el creador de la base de datos puede demostrar esa inversión, puede prohibir la extracción y/o reutilización de la totalidad o una parte sustancial del contenido de la base de datos.

Secreto empresarial y protección de intangibles: dependiendo de la tipología de Blockchain deberemos de proteger la información de una forma u otra, definiendo estrategias internas y externas del control de la información, mediante acuerdos de confidencialidad y control de acceso a aquello que se considera secreto empresarial.

> *Art. 1 Ley 1/2019, de 20 de febrero, de Secretos Empresariales: 1. El objeto de la presente ley es la protección de los secretos empresariales. A efectos de esta ley, se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.*

Identidad Digital: Utilización de Credenciales Verificables asociadas a SSI:

Esta identidad digital se relaciona con el control centralizado de los datos del interesado/ usuario. La normativa de aplicación a este ámbito reside en el propio RGPD y el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, del 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS).

Como punto de partida, el Grupo de trabajo en informe de 02.05.2019 avisan de que, aunque en Europa no se prohíbe el desarrollo de identidades digitales descentralizadas de la realidad técnica de estos avances: se debe realizar un mayor esfuerzo a nivel técnico para garantizar la seguridad y la ubicación de los datos personales.

El Reglamento eIDAS permite la creación de un mercado único electrónico europeo, regulando el mercado de emisión de certificados electrónicos cualificados o no, de firma y sello electrónico, entrega electrónica cualificada, conservación de firmas y sellos electrónicos cualificados, y validación de firmas y sellos, entre otros. Mientras que este Reglamento no establece la obligación de los Estados Miembro de notificarse para su reconocimiento mutuo transfronterizo ni tampoco regula los niveles de seguridad de estos sistemas. No obstante, el Reglamento de ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, fija las especificaciones y procedimientos teóricos mínimos para garantizar los niveles de seguridad, y el reconocimiento por parte de los demás EM cuando se haya notificado de un sistema de identificación electrónica a la Comisión Europea, según lo dispuesto en el art. 8.3 del eIDAS, estableciendo tres niveles de seguridad:

- Bajo
- Sustancia
- Alto

A nivel nacional nos encontramos con la Norma UNE 71307-1 Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de Referencia de fecha 11 de enero de 2021, norma vanguardista a nivel mundial en esta materia. Crea un comité técnico de normalización CTN 71/SC 307 de UNE.

Requisitos que debe cumplir la SSI, y la subsiguiente wallet:

- Confidencialidad que impida el acceso no autorizado

- Integridad que impida modificaciones por personas no autorizadas
- Disponibilidad que asegure el acceso confiable y oportuno a los datos o recursos para la persona apropiada.

Para ello deberemos acudir a las normas de estandarización internacionales:

- Estándares internacionales de identidad digital centralizada como los desarrollados por la Unión Internacional de Telecomunicaciones (UIT), que define la identidad como la representación de una entidad en forma de uno o más atributos que permiten que la entidad o entidades se distingan suficientemente dentro de un determinado contexto.
- ISO/IEC 24760-1:2019, esta norma determina que los dispositivos también pueden tener una identidad digital.

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital. (EIDAS2)

Vigente desde 20 de mayo de 2024 pero de aplicación progresiva con acceso por parte de los ciudadanos a las wallet para finales de 2026.

Se trata de una ampliación del marco normativa en identidad digital incluyéndose las nuevas tecnologías dando respuesta a las necesidades emergentes en este sentido, introduce la EUDI wallet, (identidad digital europea)

Esta cartera digital permitirá almacenar y gestionar múltiples credenciales electrónicas con seguridad y un grado alto de interoperabilidad entre Estados Miembros. Este Reglamento amplía la lista de servicios electrónicos de confianza incluyendo los libros mayores electrónicos.

<u>¿El código es ley? Smart Contracts y Smart Legal Contracts: No existe una normativa específica donde se regulen los SC.</u>

En inicio estableceremos el contexto del SC, debemos tener en cuenta que un SC no es lo que en derecho conocemos como contrato, se trata de código autoejecutable

independiente a las partes. ¿Estamos ante un acto jurídico? Es la cuestión por excelencia. Debemos diferenciar ambos conceptos:

La definición de Smart Contract más predominante se vincula con un programa informático que opera en una blockchain que se ejecuta de manera descentralizada a través de los nodos de la red.

Por otro lado, un Smart legal Contract sería un software desarrollado para ejecutar un contrato. Por tanto, debemos considerar que un software autosuficiente y programado para ejecutar todas o algunas de las reglas incorporadas al código; el objetivo es que los términos y condiciones del contrato sean verificables, inmutables e irrevocables. Cuando se cumplen las condiciones establecidas el SLC las aplica y automáticamente produces los efectos pactados.

Como consecuencia de lo anterior, un SC no es un acto jurídico en sí mismo, ya que conforme parte de la doctrina no existen los elementos esenciales para que se considere un contrato (capacidad, consentimiento, objeto y causa). El principal elemento para determinar si estamos ante un contrato con efectos jurídicos radica en el consentimiento estrictamente hablando, si bien nuestro CC no es claro en esta materia, si acudimos a los arts. 50 y ss del CCom encontramos algunas precisiones sobre el consentimiento.

La fórmula adecuada para que estos códigos autoejecutables sean actos jurídicos es ligarlos al lenguaje natural, dando lugar a los Smart Legal Contracts (SLC). Éstos, de conformidad con la libertad de forma general que establece nuestra normativa civil, son considerados actos jurídicos plenos:

- Art. 1261 CC: requisitos de un contrato: objeto, causa y consentimiento.
- Art, 1258 CC: perfeccionamiento del contrato por el mero consentimiento y desde ese momento obliga de lo pactado y a las consecuencias inherentes a su naturaleza de conformidad con la buena fe, el uso y la ley.
- Art. 1262 CC: los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.

Si entramos ya en entorno digital, acudimos a la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos

de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) que supone la equiparación entre los documentos en soporte papel y soporte electrónico. Así la ya mencionada LSSI en su art.24 establece que la prueba de la celebración y las obligaciones derivadas de un contrato electrónico se sujetan a las reglas generales del ordenamiento jurídico.

Además, si esos documentos van firmados electrónicamente les será también de aplicación la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Por otro lado, una novedad a tener en cuenta es el Reglamento (UE) N° 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).

- Este Reglamento establece normas armonizadas sobre la puesta a disposición de datos de productos y de servicios en favor de destinatarios, que pueden ser una persona física o jurídica, un consumidor, una empresa, una organización sin ánimo de lucro o una entidad que actúe a título profesional.

- Será aplicable a partir del 12 de septiembre de 2025.

- Contempla específicamente la definición de "contrato inteligente", entendiéndolo como "programa informático utilizado para la ejecución automatizada de un acuerdo o de parte de este, que utiliza una secuencia de registros electrónicos de datos y garantiza su integridad y la exactitud de su orden cronológico".

- Además, indica cuáles son los requisitos esenciales a los contratos inteligentes para la ejecución de acuerdos de intercambio de datos:

    - Solidez y control de acceso

    - Resolución unilateral e interrupción seguras (para evitar futuras ejecuciones accidentales)

- Archivo y continuidad de los datos (con fines de auditabilidad)
- Coherencia con las condiciones del acuerdo de intercambio de datos que ejecuta el contrato inteligente.
- Evaluación de conformidad previa sobre el cumplimiento de estos requisitos por el proveedor del contrato inteligente que, además, deberá expedir una declaración UE de conformidad.

- Debemos tener en cuenta que este Reglamento va a resultar de aplicación cuando el SLC tenga por objeto el intercambio o la puesta a disposición de información, respecto de datos personales y no personales. El significado de SLC es el mismo que hemos mencionado antes, exigiéndose tanto la materialidad en el lenguaje natural, como en el lenguaje de código; si bien, se exigen requisitos adicionales cuando el objeto sea la transmisión de información.

- Al poner los datos a disposición del tercero, el titular de los datos no debe explotar de manera abusiva su posición para buscar una ventaja competitiva en mercados en los que el titular de datos y el tercero puedan estar en competencia directa.

- Por consiguiente, el titular de los datos no debe utilizar ningún dato fácilmente disponible con el solo fin de obtener información sobre la situación económica, los activos o los métodos de producción del tercero, o en líneas generales, para socavar su posición comercial.

- El usuario debe poder compartir datos no personales con terceros con fines comerciales.

- Incluso, previo acuerdo con el usuario, los terceros pueden transmitir los derechos de acceso a otro tercero, a cambio de una compensación.

- Manifiesta la posible la nulidad de las cláusulas contractuales que sean abusivas y hayan sido impuestas unilateralmente por la empresa en relación con la protección a consumidores.

No obstante, dada la especialidad tecnológica de los SC y su ejecutabilidad automática, genera situaciones jurídico- controvertidas:

- Qué sucede con las decisiones automatizadas en relación con los derechos de protección de datos: no cabe duda de que un SC que afecte a los derechos del interesado sin consentimiento previo expreso es una actuación contraria al RGPD, y si además planteamos decisiones automatizadas, prohibidas salvo sea necesario para la celebración o ejecución de un contrato entre tú y el responsable y exista consentimiento previo, además la norma exige que el responsable garantice el derecho del interesado a obtener la intervención humana, expresar un punto de vista e impugnar la decisión. También están permitidas las decisiones automatizadas siempre que esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado. A su vez, estas excepciones no se aplicarán sobre las categorías especiales de datos (art.9.1), salvo que se aplique el artículo 9.2. letra a) o g) y se hayan tomado las medidas adecuadas citadas en el párrafo anterior.
- Qué sucede cuando el código falla. The code is law: las responsabilidades derivadas de los fallos de codificación deberán evaluarse puntualmente, ya que si es un contrato de adhesión veremos como entra en juego una responsabilidad objetiva (sin perjuicio de tener en cuenta normativa de consumidores y usuarios), mientras que si se trata de un contrato personalizado, entraríamos en la responsabilidad subjetiva del 1902 CC.
- Qué sucede si el código no falla, pero el resultado no es el que se buscaba: es una cuestión también relevante a efectos de redactar un SLC, ya que las consecuencias materiales inesperadas dan lugar a consecuencias jurídicas no deseadas.
- Qué sucede si una de las partes incumple algún pacto: es un punto conflictual habitual en los contratos y debemos llevar la aplicabilidad del 1.124 CC a los contratos autoejecutables, para salvaguarda de la propia operación autoejecutable como de los derechos y obligaciones de las partes.
- Cómo se aborda la rigidez del código con la flexibilidad interpretativa de los contratos.

Blockchain y Administración Pública: Debemos traer a colación lo que la exposición de motivos de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, establece: "*la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos, sino que debe constituir la actuación habitual de las Administraciones*". En su art.12.2 LPACAP sigue aportando garantías al uso de la tecnología en el entorno administrativo: «*Las Administraciones Públicas asistirán en el uso de medios electrónicos …especialmente en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas*».

Si bien es cierto, que hoy por hoy existe una clara prohibición en el uso de Blockchain para la identidad digital (Disp. Adicional 6ª LPACAP), no existe para otros ámbitos.

Es más, partiendo de que la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público abre la posibilidad a que las personas físicas se relaciones por medios electrónicos con la Administración (como sabes, para las personas jurídicas, es la forma obligatoria), es aquí cuando la tecnología de registro distribuido sale a la palestra. Si traemos a colación, el art. 13 de la Ley de Procedimiento Administrativo Común, esta tecnología garantizaría el acceso a la información pública garantizándose así la aplicación del principio de transparencia.

El art.14 LRJSP define por su parte la manera, el derecho y obligación de los ciudadanos al relacionarse electrónicamente con las Administraciones públicas: «*Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento*»

Por su parte el art. 40 de la misma norma establece la posibilidad de una actuación administrativa automatizada que abre la puerta a la utilización de Smart Contracts en contratación pública, en materia de ayudas y subvenciones e incluso en cuestiones de datos de salud.

En relación la ley de Contratos del Sector Público, en su Disp. Adicional decimosexta establece los criterios para la utilización de medios electrónicos, informáticos y telemáticos, en particular para la presentación de ofertas. Y si añadimos el contenido de la Disp. Adicional decimoséptima nos topamos con un cumplimiento casi completo por parte de la tecnología de cadena de bloques.

Debemos tener en cuenta que toda tecnología que vaya a ser utilizada por la Administración Pública o entidades del Sector Público debe estar sujeta a los Estándares del Esquema Nacional de Interoperabilidad.

En cuanto al uso de esta tecnología en Registros Públicos (civiles, propiedad o mercantiles, por ejemplo) habrá que modificar ciertas normativas para poder cumplir con criterios de fe pública registral o territorialidad.

b) Criptoactivos, Tokens, y NFTs

Definición amplia de criptoactivo y/o token: activo digital de origen criptográfico no tangible que suele estar registrado en registros distribuidos, que pueden tener un valor y ser la representación de un activo físico o no.
Según la Propuesta de reglamento europeo Mercados de criptoactivos que modifica la Directiva 2019/1937 un criptoactivo es «una representación digital de valor o derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar» (Reglamento MiCA art.3.1.5).

El RDL 5/2021 ofrece una definición sustancialmente idéntica, al conceptualizar los criptoactivos como «*representaciones digitales de valor o derechos que pueden transferirse y almacenarse electrónicamente, mediante la tecnología de registros distribuidos u otra similar*». Y, en la misma línea, el resto de normativa española aplicable trabaja sobre la misma definición.

En esta misma línea, debe observarse que la Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión, reconoce expresamente la posibilidad de representar valores negociables mediante tecnología de registros distribuidos, exigiendo los mismos requisitos que cuando se representan por medio de anotaciones en cuenta. Entre ellos, se encuentra la necesidad de un certificado de legitimación para

la transmisión y el ejercicio de derechos derivados de los valores negociables. Para los casos en los que se utilicen sistemas basados en esta tecnología, el documento de emisión deberá detallar los mecanismos implementados por los que se pruebe la titularidad de los derechos.

Por último, cabe destacar que, en la medida en que estemos ante un instrumento financiero sujeto a esta ley, y pese a que se utilice tecnología blockchain, la potestad de supervisión e inspección corresponde a la CNMV.

Tipología

Criptomonedas: forma más conocida y utilizada de criptoactivos. Por ejemplo, Bitcoin, Ethereum, Litecoin, y Ripple. Se utilizan para realizar pagos en línea y transferir valor de una parte a otra sin la necesidad de intermediarios financieros tradicionales.

Utility tokens: se usan dentro de una plataforma o ecosistema específico para acceder a servicios o productos específicos. Por ejemplo, los tokens de la red Ethereum que se utilizan para acceder a aplicaciones descentralizadas (dApps).

Security tokens: Representan activos financieros, como acciones o bonos, y están sujetos a regulaciones de valores. Pretenden recaudar fondos para proyectos empresariales y se venden a inversores como una forma de obtener capital.

Equity tokens: son un subtipo del anterior, que además del valor financiero su propietario ostenta ciertos derechos.

Governance tokens: son tokens que ofrecen derechos en la toma de decisiones de un proyecto.

Asset tokens: son tokens referenciados a activos reales como materias primas, inmuebles, obras de arte, etc.

Tokens no fungibles: representan activos únicos o digitales, como obras de arte u objetos de colección. Pretenden verificar la autenticidad y propiedad de los activos digitales únicos.

Tokens fungibles: son tokens fraccionables.

Privacy coins o criptoactivos centrados en la privacidad: están diseñados para proporcionar un mayor nivel de privacidad y anonimato en las transacciones. Ejemplos incluyen Monero, Zcash, y Dash.

Según el Reglamento MiCA:

Asset referenced tokens, tokens referenciados a activos o fichas referenciadas a activos: un tipo de criptoactivo que, a fin de mantener un valor estable, se referencia al valor de varias monedas fiat de curso legal, una o varias materias primas, uno o varios criptoactivos, o una combinación de dichos activos. Tokens vinculados al valor del oro, por ejemplo.

Electronic money tokens o fichas de dinero electrónico: un tipo de criptoactivo cuya principal finalidad es la de ser usado como medio de intercambio y que, a fin de mantener un valor estable, se referencia al valor de una moneda fiat de curso legal. Bitcoin, ETH, USDT, BNB, MATIC, SOL, etc

- Stablecoins: son criptomonedas estables, Tether o DAI, son ejemplos de ello. Se emiten mediante Smart Contracts con valor 1 – 1 referenciada a una moneda fiat; valor relacionado con otros criptoactivos o materias primas. Se elimina la volatilidad gracias a la vinculación del valor de la stablecoin con otro valor. Tratan de mantener la estabilidad en los mercados de criptomonedas, ya que pueden utilizarse como una forma de intercambio y almacenamiento de valor sin la volatilidad asociada con otras criptomonedas.

- CBDCs o Central Bank Digital Currency: es el dinero digital del banco central que se emite de forma electrónica. Ejemplo: Dólar digital, Euro digital, e-Yuan o yen digital. Pueden ser en base Blockchain o no. Están respaldadas por el Estado emisor. Son cripto currencies públicas.

Utility Tokens o fichas de servicio: un tipo de criptoactivo usado para dar acceso digital a un bien o un servicio, disponible mediante TRD, y aceptado únicamente por el emisor de la ficha en cuestión. Da acceso a servicios o productos específicos en una plataforma o ecosistema. Por ejemplo, pueden utilizarse para pagar las tarifas de transacción en una plataforma de intercambio descentralizada o para obtener acceso premium a una red social descentralizada. Pueden estar sujetos a regulaciones en algunos casos,

especialmente si están destinados a ser utilizados en industrias reguladas, como las finanzas o la salud. Además, la emisión y venta de tokens puede estar sujeta a regulaciones en materia de protección del consumidor y publicidad engañosa.

¿Qué se queda fuera de MiCA?

NFTs o tokens no fungibles: son tokens únicos e indivisibles y se utilizan para representar activos digitales únicos, como obras de arte, música o artículos de colección. Son diferentes de las criptomonedas porque no son intercambiables en igualdad de condiciones y cada NFT es único.

Están sujetos a regulaciones de propiedad intelectual, protección al consumidor y legislación AML/CFT, entre otras.

En cuanto a la propiedad intelectual, los creadores de NFTs deben asegurarse de que tienen los derechos de autor o licencias necesarios para los activos digitales que están tokenizando. Además, los propietarios de NFTs deben respetar los derechos de propiedad intelectual de los demás y no utilizar o vender NFTs que infrinjan los derechos de autor u otros derechos de propiedad intelectual.

En relación con la protección al consumidor, los creadores de NFTs deben asegurarse de que los compradores comprendan claramente lo que están comprando y los riesgos asociados. Por ejemplo, los compradores deben saber si están comprando derechos de propiedad intelectual, una copia única de un activo digital, o simplemente un token que representa el activo digital. También deben ser conscientes de los riesgos asociados con la propiedad de activos digitales, como la posibilidad de pérdida o robo de la clave privada que permite acceder al NFT.

En cuanto a la legislación AML/CFT, las empresas pueden estar sujetas a la legislación AML/CFT, es decir, deben cumplir con las obligaciones de identificación y verificación de sus clientes, así como llevar a cabo la debida diligencia en relación con las transacciones de NFTs. Es importante en casos en los que los NFTs representan activos valiosos, como obras de arte.

Los tipos de NTFs serían los siguientes:

- De obras de arte digitales: se usan para representar obras de arte digitales, como imágenes, videos, música y otros contenidos creativos.
- De coleccionables: representan artículos coleccionables, como tarjetas de deportes, figurillas y otros objetos físicos.
- De bienes raíces virtuales: representan bienes raíces virtuales, como terrenos o propiedades dentro de videojuegos o mundos virtuales.
- De artículos de juego: representan artículos de juego virtuales, como armas o personajes, que se pueden utilizar en juegos en línea.
- De memes y otras formas de contenido viral: representar contenido viral, como memes o tuits, que han adquirido un valor cultural o histórico significativo.
- De productos de marca: representan productos de marca, como ediciones limitadas de zapatos o ropa.

Cuestiones jurídicas de los NFTs

- Propiedad intelectual: Al representar obras de arte, música y otros activos digitales únicos, los NFTs pueden plantear cuestiones de propiedad intelectual y derechos de autor. Los creadores de NFTs deben asegurarse de que tienen los derechos de propiedad intelectual necesarios antes de crear y vender NFTs. El Juzgado de lo Mercantil N°. 9 de Barcelona, Sentencia 11/2024 de 11 Ene. 2024, Proc. 776/2022, viene a sostener que no existe uso ilegitimo en la digitalización como NFTs (en categoría de obra transformada) de las 5 obras "*Oiseau volant vers le soleil*" y "*Tète et Oiseau*" de D. Joan Miró, "*Ulls i Creu*" y "*Esgrafiats*" de D. Antoni Tàpies y "*Dilatation*" de D. Miquel Barceló, ya que supuso un uso justo, legítimo e inocuo, sino más bien al contrario ya que se dio a conocer a un mayor público a través del metaverso de dichas obras.
- Impuestos: Los NFTs se consideran activos y, por lo tanto, están sujetos a impuestos sobre la renta y sobre ganancias de capital en muchos países. Los propietarios de NFTs deben cumplir con las regulaciones fiscales y reportar sus transacciones de NFTs a las autoridades fiscales correspondientes.
- Lavado de dinero: Debido a la naturaleza anónima y descentralizada de las transacciones de criptomonedas, los NFTs pueden ser utilizados para el lavado de dinero y otras actividades ilegales. Las plataformas de NFTs deben cumplir

con las regulaciones contra el lavado de dinero y trabajar para prevenir el uso de NFTs en actividades ilegales.

- Protección al consumidor: Los NFTs pueden ser vendidos en mercados en línea y plataformas de comercio electrónico, lo que significa que los vendedores deben cumplir con las leyes de protección al consumidor y garantizar que los compradores reciban lo que se les prometió.

Security Tokens o fichas de seguridad: representan la propiedad o participación en una empresa o proyecto, y pueden estar sujetos a regulaciones de valores. En la actualidad se regulan en el Reglamento (UE) 2022/858 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) nº 600/2014 y (UE) nº 909/2014 y la Directiva 2014/65/UE (MiFID II). Se pueden tokenizar, por tanto, acciones de sociedades anónimas, bonos y otras formas de deuda y participaciones en organismos de inversión colectiva. No cabria, la tokenizacion de derechos reales sin modificaciones legislativas como la LH. El pasado 24 de marzo, el Parlamento Europeo aprobó el Reglamento sobre un régimen piloto de las infraestructuras de mercado basadas en la tecnología de registro descentralizado (Reglamento DLT) para la regulación de la comercialización y liquidación de instrumentos financieros a través de tecnologías de registro distribuido. Instrumentos financieros de su ámbito de aplicación: acciones, bonos o participaciones en organismos de inversión colectiva

Usos

Acceso a servicios y productos: utilizarse como medio de pago para acceder a servicios y productos dentro de un ecosistema determinado.

Crowdfunding: Los tokens de seguridad pueden utilizarse como una forma de recaudar fondos para proyectos empresariales. Los inversores pueden comprar tokens de seguridad a cambio de capital, lo que les otorga un interés en el proyecto.

Facilitar transacciones: Transferir valor de manera rápida y segura sin la necesidad de un intermediario. Puede ser especialmente útil en transacciones transfronterizas, ya que los tokens pueden utilizarse como una forma de evitar las restricciones de las divisas y reducir los costos de transacción.

Incentivos y recompensas: para incentivar y recompensar a los usuarios dentro de una plataforma o ecosistema determinado.

Representar activos digitales o físicos: representar activos digitales o físicos, como obras de arte o bienes raíces. Los tokens no fungibles son especialmente útiles para este propósito, ya que pueden utilizarse para verificar la autenticidad y propiedad de los activos únicos.

Cuestiones legales

Fiscalidad: la emisión y la suscripción, así como la compraventa de esta tipología de activos digitales estarán sujetas a impuestos tales como TPO AJD, Actividades Económicas, IVA o IRPF/ IS.

Obligaciones financieras: algunos criptoactivos estarán sujetos a normativa MIFID II, a mercado de valores y CNMV, por lo que habrá que analizar la tipología de token o cripto que va a ser creada, lanzada, utilizada o enajenada para analizar si cumple con la normativa o no.

Blanqueo de Capitales: Recomendaciones del Grupo de Acción financiera Internacional (GAFI), aplicabilidad de las directivas anti-blanqueo y las normas KYC (*know your customer*) y AML/CFT (anti money laundering / combating the financing of terrorism). Esto significa que deben cumplir con las obligaciones de identificación y verificación de sus clientes, así como llevar a cabo la debida diligencia en relación con las transacciones de tokens. Además, deberán constar en el Registro del Banco de España los proveedores de servicios de cambio de moneda virtual por fiat y custodios de monederos electrónicos (*hot wallets*, por ejemplo).

En este punto, es importante mencionar el Reglamento (UE) N° 2024/1624, del Parlamento Europeo y del Consejo, de 31 de mayo, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo; que será aplicable, con carácter general, desde julio 2027. Sus principales novedades son:

- Se amplía el listado de sujetos obligados (se añaden, por ejemplo, a los proveedores de servicios de criptoactivos, las plataformas crowdfunding o las personas que comercializan con bienes de gran valor.

- Se incluyen reglas más detalladas sobre la identificación del titular real, obligando a las entidades obligadas a declarar su titularidad real e inscribirla en el Registro Central de Titularidades Reales.

- Se obliga a los sujetos obligados a la designación de un "director de cumplimiento normativo de AML" (AML Manager), que deberá ser obligatoriamente miembro del órgano de administración, y de un "responsable de cumplimiento normativo de AML" (AML Officer).

- Mayor rigurosidad en la aplicación de las medidas de diligencia debida con respecto al cliente

Por otro lado, se crea la Autoridad Europea de AML/CFT (AMLA) por el Reglamento (UE) Nº 2024/1620, que desarrolla una función de coordinación, armonización y supervisión.

Consumidores y usuarios: Además, se deberán atender las directrices de publicidad, transparencia y necesidad de folleto informativo que establezca la regulación por cada tipo de activo, así como determinación del derecho de desistimiento regulado en la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores.

c) Inteligencia Artificial.

Definición amplia: disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.

Tipos de IA y usos

- Machine Learning: aprendizaje automático. Ayuda a identificar patrones. La bandeja de SPAM de tu correo electrónico es muy probable que filtre los correos aplicando este tipo de desarrollo

- Inteligencia Artificial: también conocida como IA, busca replicar o imitar razonamientos, procesos o acciones humanas.
- Deep Learning: o también llamado aprendizaje profundo. Se trata de soluciones tecnológicas que comprenden comandos y pueden realizar acciones. Analizar clientes potenciales, definir sus preferencias o incluso detectar fraudes son algunos usos de esta tecnología predictiva de comportamientos.
- Redes Neuronales: sistema de procesamiento de información que emula al cerebro humano. Los Chatbots de las grandes plataformas usan estesta solución
- Sistema Experto: solucionan conflictos determinados asemejándose al razonamiento humano. Desde el monitoreo de tareas, pasando por la planificación y la clasificación, llegando a la resolución de conflictos y generación de diagnósticos.

Marco normativo

La UE pone el foco en el desarrollo normativo uniforme a través de la Estrategia Europea de IA que prima la excelencia y la confianza en esta tecnología. El paquete incluye un Plan Coordinado sobre Inteligencia Artificia, la Comunicación sobre el fomento de un enfoque único europeo de la IA, la propuesta de Reglamento de normas armonizadas sobre la IA o Acta de IA y la evaluación de impacto pertinente. Para conseguir un marco de confiabilidad, la UE propone un marco jurídico europeo para la IA a fin de abordar los riesgos para los derechos fundamentales y la seguridad, específicos de los sistemas de IA; una Directiva sobre responsabilidad por IA: adaptación de las normas de responsabilidad a la era digital y a la IA y una propuesta de Directiva sobre responsabilidad por productos defectuosos.

El punto de partida para las obligaciones en materia de IA (Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) se centra en el riego en el uso de esta tecnología. El proveedor deberá realizar una evaluación del riesgo, controles de calidad,

documentación acreditativa de los aspectos técnicos, así como la evaluación conforme de la UE que será determinada por la Autoridad competente de cada Estado Miembro.

El conflicto jurídico actual: la responsabilidad y el tratamiento de datos personales.

En materia de responsabilidad debemos acudir a la doctrina tradicional, pues la misma solo podrá recaer sobre entes con personalidad jurídica, por lo que la determinación de la responsabilidad de los entes autónomos será objeto de controversia. En materia de privacidad, deberemos analizar el tratamiento automatizado, es decir, las decisiones automatizadas y la gestión masiva de datos.

Riesgos más relevantes según INCIBE:

- Recopilan mucha información personal para funcionar correctamente. Si no se manejan y configuran adecuadamente, pueden comprometer tu privacidad.
- La información que proporcionan puede tener sesgos, no ser precisa o incluso correcta.
- Pueden ser utilizadas para generar contenido falso o desinformación de manera rápida y convincente. Pueden crear noticias falsas, artículos o videos que aparenten ser reales, lo que dificulta que las personas distingan entre información verdadera y falsa. También manipular imágenes y videos de manera sorprendentemente realista.
- Están expuestas a ataques cibernéticos y accesos no autorizados como cualquier otro sistema. Si un atacante logra vulnerar las medidas de seguridad implementadas, puede acceder a tus datos.
- En ocasiones, las decisiones tomadas por la IA son difíciles de entender porque sus procesos son complejos. Esto dificulta que comprendas cómo se toman decisiones que te afectan a nivel de privacidad y seguridad.

Recomendaciones para ciudadanos para evitar riesgos en la privacidad relacionados con las IA (INCIBE):

- Sé consciente de qué información compartes: No compartas datos personales sensibles a menos que tengas permiso y confíes en la entidad o plataforma que lo solicita.

- Verifica la información: No confíes ciegamente en todo lo que te dice un sistema de IA. Verifica los hechos y asegúrate de que las respuestas tengan sentido.

- Cuidado con el sesgo: Recuerda que las IA pueden estar sesgadas según la información con la que se entrenan. Sé consciente de posibles prejuicios y desafía las decisiones injustas o discriminatorias.

- Utiliza extensiones de navegador con precaución: Algunas extensiones basadas en IA pueden recopilar datos para su entrenamiento. Limita el uso de estas extensiones y considera la privacidad antes de instalarlas.

- Verifica tus fuentes: No tomes la IA como una fuente absoluta de verdad. Siempre verifica los hechos consultando diferentes fuentes confiables.

- Denuncia el uso de tu información privada: Si descubres que se ha comprometido tu privacidad debido a una plataforma o sistema basado en IA, denuncia ante las autoridades competentes en materia de protección de datos, en España, la Agencia Española de Protección de Datos.

Responsabilidad penal de los sistemas de IA: a priori, en relación con los art. 5, 27, 28 y 31 el CP no cabe atribuirle personalidad jurídica a un sistema de inteligencia artificial. Por lo menos por ahora. Se entiende desde esta perspectiva una inexistencia de imputabilidad penal.

¿Quién es el responsable en caso de comisión del delito? Si el sistema de IA es entendido como inimputable (por ahora) la responsabilidad recaerá sobre el usuario (art. 17 CP) que comete un hecho delictivo utilizando esta tecnología, dejando fuera de este marco a los diseñadores o desarrolladores informáticos (art. 28) pues no serían el sujeto que realiza la acción punible. La cuestión podría verse modificada si se desarrolla un software específico para delinquir.

IA Generativa: tecnologías como Chat GPT, Gemini, DALL-E están a la orden del día. Se trata de una tecnología que utilizando sistema de aprendizaje automático mediante redes neuronales avanzadas permite crear información original a partir de datos existentes. Esa información puede ser imagen, texto, música entre otros.

En este tipo de IA es necesario tener en cuenta cuestiones normativas en relación con la alimentación de esta y los datos con los que trabajamos.

- Protección de datos: sin perjuicio de la aplicabilidad del RGPD y todos sus principios, aquí se deberá evaluar además la generación de datos (ficticios o no sensibles o no) ya que dando ciertos datos nos puede facilitar información sobre hábitos y preferencias del usuario. También se deberá tener un control sobre los datos utilizados para el entrenamiento. Se deberán tomar medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos, obtener la información que se facilita a los usuarios; la recogida de consentimientos, etc.

- Propiedad intelectual, industrial y derechos de autor: debemos diferenciarnos con los sistemas de Blockchain o DLTs en este caso pues un sistema de datos no es una base de datos. En los sistemas de IA no se almacenan datos ni la información de entrenamiento lo que hace es conservar una representación abstracta de la información volcada, por eso no cabe la protección indicada anteriormente de las bases de datos en lo que respecta a los derechos sui generis, tampoco sería objeto de patente. Aquí deberíamos entrar a valorar su protección mediante el secreto empresarial.

- Elaboración de protocolos si se decide utilizar IA generativa (y cualquier otra) en el ámbito laboral

- Análisis del objetivo en el uso de IA: valoración de los riesgos, información y formación a los trabajadores y consentimientos expresos. La Evaluación de Impacto.

- Creación del IA Officer en orden a generar una cultura de cumplimiento normativo, que documente todo lo relacionado con la Ia y sus usos, gestión de un sistema de vigilancia actualizado y resiliente, supervisión humana del sistema de IA, control y registro tanto en la pertinencia como en el uso del dato, transparencia en decisiones.

d) **Metaverso.** Breve aproximación a los usos y cuestiones legales relevantes aun sin resolver.

Definición amplia: universo virtual conectado en el que se fusionan la realidad con lo digital, a través de un espacio tridimensional en el que las relaciones se basan en la comunicación entre avatares para participar en una variedad de actividades en línea, incluyendo la interacción con otros usuarios y la transferencia de datos.

Como resultado, existe el riesgo de que se produzcan violaciones de la privacidad y la protección de datos personales, como el robo de identidad y el uso no autorizado de información personal.

Para abordar estos riesgos, es importante que las empresas y organizaciones que operan en el metaverso establezcan políticas y procedimientos sólidos de Compliance para proteger los datos personales de los usuarios. Puede incluir la implementación de medidas de seguridad de la información, la obtención de consentimiento informado para el uso de datos personales y la conformidad con las leyes y regulaciones de protección de datos aplicables.

Además, las empresas y organizaciones que operan en el metaverso también pueden estar sujetas a otras regulaciones y normas, como las leyes de propiedad intelectual, la regulación financiera y las normas de comercio electrónico. En consecuencia, el Compliance es esencial para garantizar que las empresas y organizaciones operen dentro del marco legal y ético en el metaverso y eviten sanciones y otros riesgos legales.

Algunas de las principales materias que todavía están por resolver:

Estándares técnicos y de interoperabilidad: Actualmente, el metaverso no tiene un conjunto de estándares técnicos y de interoperabilidad bien definidos, lo que dificulta la creación de un entorno virtual compartido y abierto en el que los usuarios puedan interactuar. Es esencial establecer un conjunto de estándares que permitan la creación de un entorno virtual más colaborativo y faciliten la interoperabilidad entre los diversos mundos virtuales.

Privacidad y protección de datos: El metaverso plantea desafíos significativos en términos de privacidad y protección de datos, ya que los usuarios pueden compartir una gran cantidad de información personal y confidencial en un entorno virtual. Es importante establecer políticas y normativas adecuadas para proteger los datos

personales de los usuarios y garantizar que se cumplan las leyes y regulaciones de protección de datos aplicables.

Regulación y supervisión: A medida que el metaverso se vuelve más popular y generalizado, es probable que surjan cuestiones relacionadas en este sentido. Los gobiernos y otras entidades reguladoras deberán considerar cómo abordar los riesgos asociados con el metaverso, como el blanqueo de dinero, la evasión fiscal y otros delitos. Es importante establecer políticas y regulaciones adecuadas que permitan un desarrollo seguro y sostenible.

Seguridad y ciberseguridad: Las empresas y organizaciones que operan en el metaverso deben tomar medidas adecuadas para proteger los datos y la información personal de los usuarios, así como para prevenir el acceso no autorizado y otras amenazas cibernéticas. Puede incluir la implementación de medidas de seguridad de la información, como la autenticación de usuarios y la encriptación de datos, así como la capacitación de los usuarios sobre las mejores prácticas de seguridad en línea.

Propiedad intelectual: La propiedad intelectual se refiere a los derechos que tienen las personas sobre sus creaciones, como patentes, marcas registradas y derechos de autor. En el metaverso, la propiedad intelectual puede ser un tema complicado porque las personas pueden crear y compartir contenidos, pero puede ser difícil determinar quién es el propietario de esos contenidos. Además, los usuarios del metaverso pueden copiar, modificar y distribuir contenidos de manera rápida y fácil, lo que puede hacer que sea difícil para los creadores proteger sus derechos de propiedad intelectual.

Derechos de autor: Los derechos de autor se refieren a los derechos que tienen los creadores de contenidos sobre sus obras, incluyendo textos, imágenes, música y vídeos. En el metaverso, los usuarios pueden crear contenidos que infrinjan los derechos de autor de otras personas. Por ejemplo, pueden crear una obra derivada de una obra protegida por derechos de autor o utilizar música o imágenes que no tienen licencia. Puede resultar en demandas y litigios, lo que puede ser costoso y complicado.

Responsabilidad civil: La responsabilidad civil se refiere a la responsabilidad de una persona o empresa por los daños que causan a otra persona. En el metaverso, puede ser difícil determinar quién es responsable si un usuario resulta herido o sufre daños. Por

ejemplo, si un usuario compra un objeto virtual en el metaverso y sufre daños o perjuicios a causa del objeto, puede ser difícil determinar quién es responsable, incluso la propia existencia del daño puede ser objeto de debate jurídico. Las empresas y organizaciones que operan en el metaverso deben tener en cuenta estas cuestiones y tomar medidas adecuadas para garantizar que los usuarios estén seguros y que los riesgos se gestionen adecuadamente. La línea se desdibuja aun entre la responsabilidad contractual y la extracontractual.

Protección del consumidor: Las empresas y organizaciones que operan en el espacio virtual tienen la responsabilidad de proteger a los consumidores de prácticas comerciales engañosas, fraudes y estafas. Es especialmente importante ya que, en el metaverso, los consumidores pueden ser víctimas de diversas formas de engaño, incluyendo la venta de bienes o servicios virtuales que no existen o que no cumplen con lo prometido, el robo de identidad virtual y la divulgación no autorizada de información personal.

Jurisdicción y normativa aplicable: En relación con la jurisdicción, puede ser difusa por su naturaleza virtual y global. Los límites geográficos tradicionales pueden no ser aplicables en el contexto de la propiedad virtual. Asimismo, los conflictos pueden involucrar a personas de diferentes países y jurisdicciones, lo que complica la determinación de qué leyes y regulaciones son aplicables.

En materia de ley y jurisdicción aplicable podemos acudir a los Reglamentos europeos, a falta de clausla vinculante para las partes:

- LOPJ
- Bruselas I
- Roma I
- Roma II
- Lugano II
- Convenio de Nueva York para materia arbitral.

Delitos e ilícitos administrativos en el metaverso, haciendo especial relevancia en la evaluación de riesgos. Dentro del metaverso se pueden dar delitos e ilícitos administrativos. En este ámbito lo relevante será cuestionarse si los delitos tipificados en

nuestro Código Penal pueden ser aplicados por analogía al mundo virtual. ¿Tiene la misma categoría penal un robo con violencia con resultado de muerte en el mundo físico que el mismo delito que recae sobre un avatar?

Relación entre el metaverso con el mercado, las marcas y los negocios virtuales

Ejemplos claros de la dualidad legal de ambos espacios lo vemos en las marcas de lujo y su utilización por terceros no autorizados en el metaverso.

¿El registro de marca o patente aplica también al mundo virtual? Hay multitud de marcas que están iniciando la protección de sus intangibles en el Metaverso.

Por lo tanto, es necesario establecer políticas y regulaciones que protejan a los consumidores, diseñadas para garantizar que los usuarios tengan información clara y precisa sobre los bienes y servicios que se ofrecen, incluyendo precios, términos y condiciones, y cualquier otra información relevante. También deben establecerse medidas adecuadas para proteger la privacidad y la seguridad de los datos personales de los usuarios.

Además, las empresas y organizaciones deberán estar sujetas a la supervisión y el control por parte de las autoridades regulatorias para asegurar que cumplan con las leyes y regulaciones aplicables en materia de protección del consumidor. Puede incluir la obligación de obtener licencias y permisos para operar en el metaverso, así como la obligación de cumplir con estándares de seguridad y privacidad.

La aplicación práctica del metaverso en el sector de las entidades sin ánimo de lucro.

En primer lugar, las entidades sin ánimo de lucro podrían utilizar el metaverso para organizar eventos virtuales de recaudación de fondos vendiendo bienes virtuales, como objetos de colección, para financiar sus programas y servicios.

En segundo lugar, el metaverso también podría proporcionar una plataforma para que las entidades recluten voluntarios y los involucren en proyectos y actividades virtuales.

En tercer lugar, el metaverso podría ser un espacio en el que las entidades sin ánimo de lucro puedan conectarse con otros grupos y organizaciones similares para compartir recursos, colaborar en proyectos y aumentar el impacto de su trabajo.

Por último, las entidades sin ánimo de lucro podrían utilizar el metaverso para crear campañas de concienciación sobre problemas sociales y educar a la comunidad sobre temas importantes relacionados con su causa.

e) Big data

Definición: gestión y análisis masiva de datos que ofrezca información de calidad y relevante en poco tiempo.

Protección de Datos de Carácter Personal

En primer lugar, definir la aplicabilidad o no del RGPD y la LOPDGDD: ¿la gestión masiva de datos permite la identificación, directa o indirecta, de un sujeto? ¿se consigue la anonimización? En caso negativo, aplicará la normativa.

Tendremos control sobre creación de perfiles y seguimiento de conductas de las personas

Ejercicio de derechos, en especial el de oposición y consentimiento expreso a decisiones automatizadas

Propiedad Intelectual e industrial: en este punto atenderemos al objeto de protección:

Software, algoritmos o procesadores: La Directiva 2009/24/CE sobre la protección jurídica de programas de ordenador excluye a los algoritmos de la protección otorgada por la propiedad intelectual como obras protegibles en la medida en que se trate de meras ideas y principios en los que se base un programa de ordenador. En estos casos, tras el análisis de otros aspectos de estrategia de negocio, se suele recomendar la protección mediante secreto empresarial.

Bases de datos: protección por derechos de autor como bases de datos sui generis, atendiendo a la situación contractual de quien desarrolle el producto.

f) Normativas para tener en cuenta Ley de gobernanza de Datos y la Data ActCloud computing

Definición: computación en la nube: modelo que permite ofrecer servicios de conectividad a gran escala, a través de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos.

Modelos de nubes y externalización de servicios

Públicas: infraestructuras con uso público y abierto que se gestionan por operadores de servicios en la nube. Por ejemplo: Azure, Google Cloud, Amazon Web Services...)

Privadas: infraestructuras solo disponibles para una organización o entidad de pago. Pueden ser propias o por un CPS.

Comunitarias: el acceso a la infraestructura es exclusivo de una comunidad especifica de entidades.

Hibridas: sus infraestructuras se componen por dos o más tipos de nubes.

Principales riesgos:

Brechas de seguridad e incumplimiento de normativas de seguridad del dato: puede producirse de forma accidental o de forma malintencionada, y puede producirse perdidas duraderas o temporales. Analizar el nivel de servicio de proveedores para evaluar criterios de recuperación, copias de seguridad y migración de datos. Además, es obligatoria la realización de copias de seguridad con periodicidad semanal, garantizando la restauración de datos al momento anterior a la pérdida y backup remoto. La redacción de contratos adecuados que recojan clausulas relacionadas con SLA (Service Level Agreement), o acuerdo de nivel de servicio; privacidad y protección de datos; posibilidad del responsable del tratamiento de auditar las medidas de seguridad del proveedor del servicio cloud; confidencialidad de la información; garantías de acceso a la información; propiedad intelectual; responsabilidad; resolución anticipada; ley aplicable y jurisdicción; mecanismos de resolución de conflictos.

g) IoT

Definición: internet de las cosas hace referencia a la interconectividad a través de internet de objetos cotidianos, que pueden registrar, procesar, almacenar o transferir información.

No existe un marco normativo regulador. No obstante, la normativa de referencia:

- Grupo de Trabajo del artículo 29, Dictamen 8/2014
- Estándares de ENISA
- Publicaciones de AEPD en la materia.

Implicaciones en privacidad que variaran dependiendo del tipo de dispositivo y la tipología de datos que trate.

No será lo mismo una Alexa o un sistema integrado con IA que capte movimientos oculares y que sustraigan datos neurosensibles.

Usos: Smart cities, mejora la experiencia cliente, domótica, etc

h) Sandboxes e innovación

El sandbox es un espacio de prueba controlado para las tecnologías emergentes.

Existen diversos tipos de sandboxes en materia financiera y privacidad, si bien en España se regulan mediante la ley 7/2020, para la transformación digital del sistema financiero.

Resolución de 28 de junio de 2024 de la Secretaría General del Tesoro y Financiación Internacional por la que se convoca el acceso a la octava cohorte del espacio controlado de pruebas (sandbox) previsto en la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero.

3. La transformación digital del Tercer Sector

La transformación digital aparece como un elemento necesario de adaptación para las entidades sin ánimo de lucro que quieran permanecer en el tiempo, llegar a nuevos sectores sociales y, en consecuencia, conseguir sus objetivos sociales.

Desde la creación de la página web a la inclusión en Metaversos, pasando por procesos de automatización, gestión de información o transacciones económicas, entre otras muchas posibilidades, es necesario tener en cuenta los factores legales y el impacto que la digitalización tiene para sus sistemas de compliance.

Concepto: es un proceso en el que la organización reorienta su actividad hacia el uso eficiente de las tecnologías emergentes, con el objetivo de obtener una mejora en sus servicios, procesos internos y externos. En búsqueda de una organización más fuerte y perdurable en el tiempo.

Supone un cambio cultural que deberá ir acompañado de la formación en competencia digitales de toda la estructura, reorganizando dicha estructura hacia una incorporación paulatina de aquellas aplicaciones tecnológicas que tengan sentido real y rechazar otras que no aporten valor.

a) <u>Detección de riesgos y cómo evitarlos con NNTT.</u>

- Corporativos: aquellos relacionados con la estructura legal de la organización.
- Riegos de activos: protección de los valores tangibles e intangibles.
- Contractuales: riesgos asumidos por asumir obligaciones y deberes.
- Litigiosidad: evaluación de la litigiosidad
- Regulación: infracciones y sanciones por incumplimiento de normativa.
- Territoriales y jurisdiccionales. Normativa aplicable y resolución de conflictos.
- Constitutivos y extintivos: aquellos relacionados con la creación y disolución de la sociedad sin ánimo de lucro.

b) <u>Nuevas estafas, delitos y fraudes</u>

- Suplantación de identidad de entidades autorizadas
- Cuentas de trading financiadas
- Fraude del técnico informático
- *Recovery room*
- Fraudes con criptoactivos
- Esquema ponzi
- Phising
- Smishing
- Vishing

- Pharming
- Fraude financiero en RRSS
- Secuestro de DNS
- Delito de intrusismo informático (Hacking) artículo 197 bis 1 del Código Penal
- Interceptación ilegítima de comunicaciones entre sistemas de información artículo 197 bis 2 del Código Penal
- Facilitación de herramientas informáticas para la comisión de los delitos anteriores
- Daños informáticos (cracking) artículo 264 del Código Penal
- Obstaculización o interrupción de un sistema informático artículo 264 bis del Código Penal
- Delito de facilitación de herramientas informáticas para facilitar la comisión de los delitos anteriores artículo 264 ter del Código Penal
- Descubrimiento y revelación de secretos artículo 197 del Código Penal
- Delitos contra la propiedad intelectual, industrial artículos 270 a 277
- Delitos contra el mercado artículos 278 a 286
- Delitos de falsificación o suministro de medicamentos sin autorización artículo 361 bis del Código Penal
- Falsedades del art. 400 CP
- Delitos de odio y discriminación art. 510.3 CP
- Delitos de terrorismo art 575.2 CP
- Delitos de acoso, deepfakes, ciberbullyng, chantajes, ingeniería social, reconocimiento facial, encubrimiento digital, usurpación de identidad, vulneración de la reputación *online*, estafas cibernéticas, delitos contra la integridad moral y sexual, etc.

c) <u>Prevención de estafas y fraudes en el Tercer Sector</u>

- Sistemas de compliance integrales, revisión y actualización constante
- Formación e información continuada al personal laboral y mercantil.
- Sistemas de seguridad actualizados
- No utilización de softwares piratas o sin licencias y siempre con las ultimas actualizaciones
- Gestión de claves
- Cifrado de datos

- Copias de seguridad
- Control de dispositivos conectados
- Redacción de cláusulas contractuales
- etc

Material de consulta y enlaces de interés:

Guía Estafas y fraudes CNMV

Breifing, Metaverse. Opportunities, sisk and policy implications. EPRS | European Parliamentary Research Service Authors: Tambiama Madiega, Polona Car and Maria Niestadt with Louise Van de Pol Members' Research Service PE 733.557 – June 2022

Guías de AEPD

Guías INCIBE

https://www.coindesk.com/es/opinion/2024/10/18/the-new-blockchain-trilemma-is-here-and-its-not-about-technology/

https://www.ibm.com/es-es/topics/blockchain-for-good

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf

https://www.incibe.es/ciudadania/blog/inteligencia-artificial-ia-que-es-ventajas-y-riesgos

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.tesoro.es/sites/default/files/sandbox/report_Resoluci%C3%B3n%20de%20convocatoria%20de%20la%208%C2%AA%20cohorte%20del%20Sandbox.pdf