BLOQUE 8: Compliance, digitalización y nuevas tecnologías

Sesiones 11 y 12 (14 y 21 de junio de 2023)
Cómo aplicar las nuevas tecnologías a nuestro sistema de compliance

- *C. Yvonne Mähler Lucini*
- *Mar Sanz (Centro de Estudios Garrigues)*

Fundación Pro Bono España

CENTRO DE ESTUDIOS GARRIGUES

Fundación Nemesio Diez

I. 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

TIPOS	
• **Compliance para el compliance**	• **Compliance para la digitalización**

II. BLOCKCHAIN

1. Qué es, cómo funciona y usos

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.

Tecnología que soporta el registro descentralizado de datos cifrados

Tipología de las tecnologías de registro distribuido (DLT) que concatena bloques en orden, vinculados entre sí y protegidos por pruebas criptográficas.

- Resuelve el Trilema de la Blockchain
  - **Descentralización:** No hay control central sobre la estructura.
    - Los nodos tienen acceso a los mismos datos —> la cadena de bloques permite que la creación de nuevos bloques se realice con la información contenida en los anteriores.
  - **Seguridad**: Más conflicto —> la descentralización fomenta ataques indeseados.
    - Solución: protocolos de consenso y sistemas criptográficos.
  - **Escalabilidad**: crecimiento exponencial de la estructura y aceptar cada vez más transacciones

1.1 Tipologías de Blockchain

Pública	Cualquier persona puede unirse libremente a la red sin permisos, pudiendo ver, participar y validar transacciones. Se prima la transparencia y descentralización Los participantes se denominan **mineros** —> minan los bloques a cambio del token o criptomoneda **Código**: *open source* o abierto
Privada	El acceso se limita y restringe, por lo que los participantes están autorizados previamente. Prima la seguridad frente a la descentralización y la transparencia.
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.
Híbrida	Red que une características de las dos primeras. • Privado: participación • Público y verificable: el registro transaccional

1.2 Protocolo de consenso

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: bitcoin • Proof of stake: Ethereum • Proof of importance • Ouroboros	• Proof of burn • Proof of capacity • Proof of authority • Otras que se desarrollen

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

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

3. 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.

4. Normativas que deben ser tenidas en cuenta

Protección de datos de carácter personal

Evaluación del impacto:
- art. 35 RGPD: La hará el responsable del tratamiento cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.
- Encriptación de la información almacenada en los nodos: determinar si es anonimizada o seudonimizada.
  - Hashing→ técnica de seudonimización y sujeta a la aplicación del RGPD.
- 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.

- Protege la inversión sustancial
- Protege el contenido económico de las creaciones: evitando que terceros exploten económicamente esas bases de datos
- Si el creador demuestra la inversión, puede prohibir la extracción / reutilización de toda o una parte sustancial del contenido de la base de datos

Secreto empresarial y protección de intangibles

Dependiendo de la tipología de Blockchain se habrá de proteger la información de una forma u otra

Identidad Digital

Uso de Credenciales Verificables asociados a SSI:

- Relación con el control centralizado de los datos del interesado / usuario.
- **RGPD** y el **Reglamento (UE) No 910/2014** del Parlamento Europeo y del Consejo, del 23 de julio de 2014
- **Informe de 02.05.2019**: mayor esfuerzo a técnico para garantizar la seguridad y la ubicación de los datos personales.
- **Reglamento eIDAS**: creación de un mercado único electrónico europeo.
- **Reglamento de ejecución (UE) 2015/1502** —> 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. Niveles de seguridad:
  - Bajo
  - Sustancial
  - Alto

Esfera nacional

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 ha de cumplir la SSI

- 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

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

- Código autoejecutable independiente a las partes
- No es un acto jurídico. Para que lo sean —> ligarlos al lenguaje natural, dando lugar a los Smart Legal Contracts
- Según el Código Civil son considerados actos jurídicos plenos: artículos 1261, 1258 y 1262 del Código Civil

Entorno digital: **Directiva 2000/31/CE** supone la equiparación entre los documentos en soporte papel y soporte electrónico.

Aplicación **Ley 6/2020**, de 11 de noviembre —> documentos firmados electrónicamente

Dada la especialidad tecnológica de los SC y su ejecutabilidad automática, genera situaciones jurídico- controvertidas:

- Decisiones automatizadas en relación con los derechos de protección de datos
- Fallo del código
- No fallo del código pero resultado diferente al buscado
- Incumpliendo de las partes de algún pacto

Blockchain y Administración Pública

Ley 39/2015: "*la tramitación electrónica (…) debe constituir la actuación habitual de las Administraciones*".

En su **art.12.2 LPAC** aporta garantías al uso de la tecnología en el entorno administrativo: "(…) *en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas*».

No existe una clara prohibición en el uso de Blockchain para la identidad digital (Disp. Adicional 6a LPAC), no existe para otros ámbitos.

La Ley 40/2015: abre la posibilidad a que las personas físicas se relaciones por medios electrónicos con la Administración

El **art.14 LRJSP** define por su parte la manera, el derecho y obligación de los ciudadanos al relacionarse electrónicamente con las Administraciones públicas:

Ley de Contratos del Sector Público: criterios para la utilización de medios electrónicos, informáticos y telemáticos, en particular para la presentación de ofertas. u.

Toda tecnología 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**: modificar ciertas normativas para poder cumplir con criterios de fe pública registral o territorialidad.

III. CRIPTOACTIVOS, TOKENS Y NFTs

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.

Propuesta MiCA

Representación digital de valor o derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología similar

RDL 5/2021

Representaciones digitales de valor o derechos que pueden transferirse y almacenarse electrónicamente, mediante la tecnología de registros distribuidos u otra similar

III. Criptoactivos, Tokens, y NFTs

Criptomonedas	Realizar pagos en línea y transferir valor de una parte a otra sin la necesidad de intermediarios financieros tradicionales. Bitcoin, Ethereum
Utility tokens	Para acceder a servicios o productos específicos. Tokens de la red Ethereum
Security tokens	Representan activos financieros, como acciones o bonos, y están sujetos a regulaciones de valores.
Equity tokens	Subtipo del anterior, que además del valor financiero su propietario ostenta ciertos derechos
Governance tokens	Ofrecen derechos en la toma de decisiones de un proyecto
Asset 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. NFTs
Tokens fungibles	Tokens fraccionables. Bitcoin
Privacy coins	Diseñados para proporcionar un mayor nivel de privacidad y anonimato en las transacciones. Zcash, Dash

III. Criptoactivos, Tokens, y NFTs

Reglamento MiCA

Asset referenced tokens, tokens referenciados a activos o fichas referenciadas a activos	Con la finalidad 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	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 - CBDCs o Central Bank Digital Currency. Dólar digital, Euro digital, e-Yuan o yen digital
Utility Tokens o fichas de servicio	Concede 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.

III. Criptoactivos, Tokens, y NFTs

¿Qué se queda fuera de MiCA?

NFTs	- Propiedad intelectual - Protección al consumidor - Legislación AML/CFT - Impuestos
Security Tokens o fichas de seguridad	- 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). - Acciones de sociedades anónimas, bonos y otras formas de deuda y participaciones en organismos de inversión colectiva. - No derechos reales sin modificaciones legislativas como la LH. - Fiscalidad - Obligaciones financieras - Blanqueo de capitales - Consumidores y usuarios

III. Criptoactivos, Tokens, y NFTs

Ejemplos de uso de los criptoactivos

Acceso a servicios y productos	Crowdfunding	Facilitar transacciones	Incentivos y recompensas	Representar activos digitales o físicos
Medio de pago	Recaudación fondos	Medio de pago	Servicio o producto dentro de un ecosistema	NFTs

Dependiendo la utilidad y el destino del token se aplicará una normativa u otra→ necesario estudio de los riesgos y adaptación normativa

IV. 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.

Inteligencia Artificial	Machine Learning	Deep Learning	Redes Neuronales	Sistema Experto
Replicar o imitar razonamientos, procesos o acciones humanas	Aprendizaje automático	Aprendizaje profundo	Emula al cerebro humano	Razonamiento humano

- Aplicaciones que violan derechos humanos fundamentales:
  sistemas de puntuación social, vigilancia masiva, identificación biométrica a distancia, manipulación del comportamiento causando daños…
- Evaluación de conformidad:
  Acceso a empleo, educación y servicios públicos, componentes de seguridad de vehículos, aplicación de la ley, etc
- Obligación de transparencia:
  Suplantación de personalidad, chatbots, reconocimiento de emociones, Deep fakes, categorización biométrica, etc.
- Sin obligaciones
  Resto de usos

V. METAVERSO. BREVE APROXIMACIÓN A LOS USOS Y CUESTIONES LEGALES RELEVANTES AUN SIN RESOLVER

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.

Riesgo: violaciones de la privacidad y de la protección de datos personales

¿Cómo abordarlos?

- Políticas y procedimientos sólidos de Compliance
- Medidas de seguridad de la información
- Consentimiento informado para el uso de datos personales
- Conformidad con las leyes y regulaciones de protección de datos personales

V. METAVERSO. BREVE APROXIMACIÓN A LOS USOS Y CUESTIONES LEGALES RELEVANTES AUN SIN RESOLVER

ESTÁNDARES TÉCNICOS Y DE INTEROPERABILIDAD	PRIVACIDAD Y PROTECCIÓN DE DATOS	REGULACIÓN Y SUPERVISIÓN	SEGURIDAD Y CIBERSEGURIDAD
• Inexistencia de estándares técnicos y de interoperabilidad bien definidos • Dificulta la creación de un entorno virtual compartido y abierto • Esencial: crear estándares que permitan la creación de un entorno virtual más colaborativo	Los usuarios pueden compartir información personal y confidencial en un entorno virtual Políticas y normativas adecuadas para proteger los datos personales y garantizar que se cumplan las leyes y regulaciones de protección de datos aplicables	Gobierno y entidades reguladoras Cómo abordar los riesgos asociados con el metaverso: • Blanqueo de dinero • Evasión fiscal	Las empresas y organizaciones Tomar medidas para: • proteger los datos y la información personal de los usuarios • Prevenir el acceso no autorizado y otras amenazas cibernéticas

V. METAVERSO. BREVE APROXIMACIÓN A LOS USOS Y CUESTIONES LEGALES RELEVANTES AUN SIN RESOLVER

PROPIEDAD INTELECTUAL	DERECHOS DE AUTOR	RESPONSABILIDAD CIVIL	PROTECCIÓN DEL CONSUMIDOR
Derechos de las personas sobre sus creaciones (patentes, marcas registradas y derechos de autor) **Metaverso**: personas crean y comparten contenido - dificultad para determinar la propiedad - Usuarios: copiar, modificar y distribuir el contenido rápida y facilmente	Derechos de los creadores de contenidos sobre sus obras Metaverso - crear contenido que infrinja los derechos de autor de otras personas	Responsabilidad de una persona / empresa por los daños causados a otra persona. **Metaverso**: difícil determinar el responsable si un usuario es herido o sufre daños. <u>Ejemplo</u> Usuario compra un objeto virtual y sufre daños a causa del objeto —> difícil determinar el responsable.	Las empresas y organizaciones han de proteger a los consumidores de prácticas comerciales engañosas, fraudes y estafas

V. METAVERSO. BREVE APROXIMACIÓN A LOS USOS Y CUESTIONES LEGALES RELEVANTES AUN SIN RESOLVER

JURISDICCIÓN Y NORMATIVA APLICABLE	DELITOS E ILÍCITOS ADMINISTRATIVOS	EL MERCADO Y EL METAVERSO, LAS MARCAS Y LOS NEGOCIOS VIRTUALES
Jurisdicción: difusa por su naturaleza virtual y global. **Límites geográficos tradicionales:** pueden no aplicarse en el contexto de la propiedad virtual. **Conflictos**: pueden involucrar a personas de diferentes países y jurisdicciones —> complicación a la hora de determinas la ley y regulación aplicable	Cuestionarse si los delitos tipificados en el Código Penal pueden aplicarse 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?	**Dualidad legal:** marcas de lujo y su uso por terceros no autorizados en el metaverso ¿El registro de marca o patente aplica también al mundo virtual? Multitud de marcas que están iniciando la protección de sus intangibles en el Metaverso. Necesario políticas y regulaciones para proteger a los consumidores y medidas adecuadas para proteger la privacidad y seguridad de los datos personales.

V. METAVERSO. BREVE APROXIMACIÓN A LOS USOS Y CUESTIONES LEGALES RELEVANTES AUN SIN RESOLVER

2. La aplicación práctica del Metaverso en las entidades sin ánimo de lucro

1. **Organización de eventos virtuales** de recaudación de fondos: venta de bienes virtuales para financiar programas y servicios.
2. Proporcional una plataforma para que recluten **voluntarios** y los involucren en **proyectos y actividades virtuales**
3. Conexión con otros grupos organizaciones similares para:
    1. **Compartir** recursos,
    2. **Colaborar** en proyectos y
    3. **Aumentar el impacto** de su trabajo
4. Crear compañas de **concienciación** sobre problemas sociales y educar a la comunidad sobre temas importantes relacionados con su causa

VI. 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	¿La gestión masiva de datos permite la identificación, directa o indirecta, de un sujeto?
Security Tokens o fichas de seguridad	- Software, algoritmos o procesadores: Directiva 2009/24/CE sobre la protección jurídica de programas de ordenador - Bases de datos: derechos de autor como bases de datos sui generis

VII. CLOUD 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.

Públicas	Infraestructuras con uso publico y abierto que se gestionan por operadores de servicios en la nube
Privadas	Infraestructuras solo disponibles para una organización o entidad de pago. Pueden ser propias o por un CPS
Comunitarias	Acceso a la infraestructura es exclusivo de una comunidad especifica de entidades
Híbridas	Sus infraestructuras se componen por dos o más tipos de nubes

Brechas de seguridad e incumplimiento de normativas de seguridad del dato

Nivel de servicio

Copias de seguridad

Migracion de datos

Cláusulas SLA

VIII. 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

The Cyber Resilience Act - CRA
Directiva NIS2
ENISA (Agencia de la Unión Europea para la Ciberseguridad)
Estándar ISO/IEC 30141 Internet de las Cosas (IoT)- Arquitectura de Referencia
ISO/IEC 27400 e ISO/IEC 27402 para la ciberseguridad y privacidad del IoT
ISO/IEC 21823: las normas de la interoperabilidad
Estándares del Instituto de Ingenieros Eléctricos y Electrónicos

NORMATIVA DE REFERENCIA

Grupo de Trabajo del artículo 29, Dictamen 8/2014

Estándares de ENISA

Publicaciones de AEPD en la materia.

Publicaciones INCIBE

IX. SANDBOXES E INNOVACION

Definición: Un espacio de pruebas controlado o sandbox es un entorno en el que empresas del sector tecnológico o financiero que están desarrollando tecnologías novedosas pueden probar de forma segura sus propuestas.

ley 7/2020, para la transformación digital del sistema financiero	El entorno controlado y delimitado de pruebas regulado por el Título II de esta Ley y por los correspondientes protocolos que amparan la realización de una o varias pruebas de innovación financiera de base tecnológica aplicable en el sistema financiero, incluidas en un proyecto piloto
Real Decreto Sandbox IA	Entorno controlado, con una duración determinada, que proporciona un contexto estructurado para el desarrollo de las actuaciones necesarias que posibiliten a los sistemas de inteligencia artificial de alto riesgo cumplir con los requisitos establecidos en este Real Decreto, bajo la supervisión del órgano competente

X. TRANSFORMACION DEL TERCER SECTOR

Detección de riesgos y cómo evitarlos con NNTT	Nuevas estafas y fraudes	Prevención de estafas y fraudes en el tercer sector
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.	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	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

BLOQUE 8: Compliance, digitalización y nuevas tecnologías

Sesiones 11 y 12 (14 y 21 de junio de 2023)
Cómo aplicar las nuevas tecnologías a nuestro sistema de compliance

- *C. Yvonne Mähler Lucini*
- *Mar Sanz (Centro de Estudios Garrigues)*

MUCHAS GRACIAS

Fundación Pro Bono España

CENTRO DE ESTUDIOS GARRIGUES

Fundación Nemesio Diez