Week 3 - Regolazione e tutela dei beni digitali

Introduzione: Dal "cosa" al "come" – governare il valore digitale

Superata la domanda sul "cosa" siano questi beni, l'analisi si concentra sul "come": come vengono regolati, protetti e governati. Il mondo giuridico sta elaborando una duplice e complementare risposta. Da un lato, la *lex publica*, il diritto imperativo dei mercati, incarnato dal Regolamento europeo MiCAR, mira a garantire stabilità, trasparenza e protezione degli investitori. Dall'altro, una nuova *lex privata* o *lex mercatoria digitale*, rappresentata dai Principi UNIDROIT, cerca di creare un linguaggio comune e flessibile per la circolazione transfrontaliera dei diritti su questi beni.

Tale linguaggio comune sta prendendo la forma di un approccio multi-livello, che armonizza regolamentazioni pubbliche, come il MiCAR, principi di soft law internazionale (UNIDROIT), strumenti privatistici tradizionali adattati al nuovo contesto (il trust) e forme di autotutela tecnologica (Multi-Sig, MPC).

Il Regolamento (UE) 2023/1114 (MiCAR).

Architettura e finalità del MiCAR.

Il Regolamento (UE) 2023/1114, noto come MiCAR (Markets in Crypto-Assets), rappresenta la prima e ad oggi più completa iniziativa legislativa a livello globale per creare un quadro normativo armonizzato per le cripto-attività. Gli obiettivi dichiarati sono molteplici e interconnessi: fornire certezza giuridica per promuovere l'innovazione, tutelare i consumatori e gli investitori, preservare l'integrità del mercato e garantire la stabilità finanziaria. La scelta di utilizzare un regolamento, atto direttamente applicabile in tutti gli Stati membri, e di fondarlo sull'articolo 114 del Trattato sul Funzionamento dell'Unione Europea (TFUE) — la base giuridica per l'armonizzazione del mercato interno — segnala la chiara ambizione di creare un mercato unico europeo per i servizi legati alle cripto-attività, con un regime di "passaporto europeo" per gli operatori autorizzati.

Il perimetro regolamentare.

Il MiCAR adotta un approccio tassonomico, distinguendo tre categorie principali di cripto-attività, classificate in base al meccanismo di stabilizzazione del loro valore:

1. **Asset-Referenced Tokens (ART):** Token che mirano a mantenere un valore stabile facendo riferimento a un valore o a un diritto, oppure a una loro combinazione, incluso un paniere di una o più valute ufficiali, una o più commodity, o una o più cripto-attività.
2. **E-money Tokens (EMT) o Token di Moneta Elettronica:** Token che mirano a

mantenere un valore stabile facendo riferimento al valore di una sola valuta ufficiale avente corso legale.
3. **"Altre Cripto-attività":** Categoria residuale che include tutte le cripto-attività diverse da ART ed EMT, come gli utility token, e che non rientrano nella definizione di strumenti finanziari ai sensi della direttiva MiFID II.

Sono invece esplicitamente fuori dal suo ambito di applicazione le cripto-attività che sono uniche e non fungibili (NFT), a meno che non siano emesse in grandi serie o raccolte che, di fatto, ne suggeriscano la fungibilità. La mera attribuzione di un identificativo unico non è sufficiente a qualificare un asset come non fungibile; anche il bene o diritto sottostante deve essere unico. Sono inoltre escluse le cripto-attività per le quali non vi è un emittente identificabile (come Bitcoin) e, aspetto cruciale, i servizi per le cripto-attività prestati in modo completamente decentralizzato, ovvero senza alcun intermediario (il mondo della Finanza Decentralizzata o DeFi).

Questa scelta del legislatore europeo è eminentemente pragmatica. Anziché tentare di regolare l'irregolabile — un protocollo puramente decentralizzato privo di un soggetto giuridico di riferimento — ha scelto di concentrarsi sui "punti di contatto" tra l'ecosistema cripto e l'economia tradizionale: gli emittenti identificabili e i prestatori di servizi centralizzati (CASP). Questa strategia rende il regolamento concretamente applicabile e la vigilanza da parte delle autorità nazionali possibile. Tuttavia, crea inevitabilmente un "donut hole" regolamentare. La DeFi pura, in cui i servizi sono forniti direttamente da smart contract autonomi senza un intermediario identificabile, resta formalmente al di fuori del perimetro di MiCAR. Ciò significa che il regolamento disciplina le “rampe di accesso e di uscita” (gli exchange, i custodi, gli emittenti di stablecoin) ma non il "cuore" decentralizzato dell'innovazione e del rischio. La conseguenza a lungo termine potrebbe essere una biforcazione del mercato: da un lato, un settore regolamentato, "sicuro" e integrato con la finanza tradizionale, attraente per gli investitori retail e istituzionali; dall'altro, un settore non regolamentato, più rischioso ma potenzialmente più innovativo e accessibile a operatori più sofisticati.

Un ecosistema di obblighi per emittenti e intermediari.

Il MiCAR impone un corpus di obblighi stringenti sia per chi emette cripto-attività sia per chi presta servizi ad esse collegati.

Per gli **emittenti**, l'obbligo cardine è che devono essere costituiti come persone giuridiche. L'adempimento centrale è la redazione e pubblicazione di un **White Paper**, un documento informativo dettagliato che deve descrivere in modo corretto, chiaro e non fuorviante le caratteristiche, i diritti, gli obblighi e i rischi associati alla cripto-attività.

L'emittente è responsabile civilmente per i danni causati a un possessore a causa di informazioni incomplete, non chiare o fuorvianti contenute nel White Paper.

Per gli emittenti di **ART e EMT**, considerati potenzialmente più rischiosi per la stabilità finanziaria, gli obblighi sono ancora più severi. Essi devono ottenere un'autorizzazione specifica, mantenere costantemente una **riserva di attività** liquida e a basso rischio, segregata e custodita, a copertura del 100% delle passività verso i possessori dei token. Devono inoltre dotarsi di **piani di risanamento e rimborso** per gestire eventuali crisi.

Per i **prestatori di servizi per le cripto-attività (CASP - Crypto-Asset Service Providers)**, il Titolo V del MiCAR introduce un regime autorizzativo completo. I CASP devono ottenere un'**autorizzazione** da un'autorità nazionale competente per poter operare nell'Unione. Una volta ottenuta, l'autorizzazione beneficia del principio del "passaporto europeo", consentendo al CASP di offrire i propri servizi in tutti gli Stati membri. Sono soggetti a **requisiti prudenziali**, che possono consistere nel mantenimento di fondi propri minimi permanenti o, in alternativa, nella stipula di una polizza assicurativa adeguata a coprire i rischi derivanti dalla loro attività. Devono inoltre rispettare rigorose **regole di condotta**, tra cui l'obbligo di agire in modo onesto, equo e professionale nell'interesse dei clienti, gestire i conflitti di interesse e garantire la custodia sicura degli asset e dei fondi dei clienti. In Italia, il decreto di adeguamento ha designato la Banca d'Italia e la Consob come autorità competenti per la vigilanza sui diversi aspetti del regolamento e ha istituito un regime transitorio per consentire ai VASP (Virtual Asset Service Providers) già iscritti nel registro speciale tenuto dall'OAM di continuare a operare a determinate condizioni, mentre presentano domanda per diventare CASP autorizzati.

Vigilanza e abusi di mercato

Il MiCAR istituisce un'architettura di vigilanza a più livelli. Le autorità nazionali competenti (in Italia, Consob e Banca d'Italia) sono responsabili della vigilanza diretta su emittenti e CASP. A livello europeo, l'Autorità Bancaria Europea (ABE) e l'Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA) hanno poteri di coordinamento, emanano standard tecnici e possono intervenire direttamente nel caso di ART ed EMT "significativi" che potrebbero porre rischi alla stabilità finanziaria dell'Unione.

Una delle innovazioni più rilevanti del regolamento è l'estensione della disciplina sugli **abusi di mercato** al mondo delle cripto-attività. Vengono introdotte norme specifiche per prevenire e sanzionare l'abuso di informazioni privilegiate (*insider dealing*) e la manipolazione del mercato, colmando una grave lacuna normativa che aveva finora caratterizzato questo settore.

La proposta della *Lex Mercatoria* digitale – I Principi UNIDROIT sui Digital Assets

Natura e Funzione dei Principi

In aggiunta alla normativa europea, i **Principi UNIDROIT sugli Asset Digitali** (maggio 2023) costituiscono un riferimento di soft law a carattere transnazionale. Sebbene non direttamente vincolanti, essi operano come raccomandazioni rivolte a legislatori e operatori del diritto, perseguendo un approccio di neutralità sia tecnologica che giurisdizionale. L'intento primario è l'istituzione di un impianto concettuale duttile, atto a incrementare la certezza del diritto, la prevedibilità e l'efficienza delle transazioni transfrontaliere che coinvolgono asset digitali, contribuendo così alla riduzione dei costi operativi e alla facilitazione del commercio su scala globale.

L'Innovazione Concettuale: dal Dominio al "Controllo"

Il cuore concettuale dei Principi UNIDROIT risiede nell'elaborazione della nozione di **"controllo"**, definita nel Principio 6. A differenza della "proprietà", il controllo non è definito come un diritto soggettivo astratto, ma come una **situazione di fatto**, una capacità funzionale e tecnicamente verificabile. Secondo i Principi, una persona ha il controllo di un asset digitale se il protocollo o il sistema sottostante le conferisce la capacità fattuale ed **esclusiva** di: (i) ottenere sostanzialmente tutti i benefici dall'asset (controllo positivo); (ii) impedire ad altri di ottenerli (controllo negativo); e (iii) trasferire ad altri tale insieme di capacità.

Questa scelta rappresenta un'operazione di ingegneria giuridica di notevole pragmatismo. Consapevole delle profonde divergenze tra civil e common law sulla nozione di proprietà applicata ai beni immateriali, UNIDROIT ha strategicamente evitato di definire l'asset digitale come "bene" o "proprietà", una qualificazione che sarebbe stata inevitabilmente divisiva e complessa, spostando invece il focus dal titolo giuridico astratto (*dominium*) alla relazione fattuale e funzionale con l'asset (*controllo*).

Il "controllo" diventa così il corrispettivo funzionale del "possesso" per i beni materiali. È un concetto che un giudice o un arbitro, in qualsiasi ordinamento, può accertare sulla base di prove tecniche (chi detiene la chiave privata? chi ha la capacità tecnica di eseguire una transazione?), senza dover prima risolvere la complessa questione dogmatica della natura proprietaria dell'asset. In questo modo, i Principi creano un ponte concettuale tra sistemi giuridici diversi e, soprattutto, tra il mondo on-chain (la realtà tecnica del controllo) e il mondo off-chain (le conseguenze giuridiche che da tale

controllo discendono). Questo approccio funzionale è un esempio di come la *soft law* possa facilitare il commercio globale superando ostacoli dogmatici nazionali.

Pilastri per un Mercato Transfrontaliero

Basandosi sul concetto di controllo, i Principi ergono alcuni pilastri fondamentali per un mercato degli asset digitali sicuro e prevedibile.

- **Tutela nella Custodia (Principio 13):** Viene sancita una regola essenziale per la fiducia degli investitori. Gli asset digitali detenuti da un custode per conto di un cliente costituiscono un patrimonio separato, non fanno parte della massa fallimentare del custode e non sono aggredibili dai suoi creditori personali in caso di insolvenza. Questo principio di segregazione patrimoniale è cruciale per la protezione degli investitori che si affidano a intermediari.
- **Acquisto in Buona Fede (Principio 8):** I Principi introducono una regola di *innocent acquisition*. Un acquirente che ottiene il controllo di un asset digitale a titolo oneroso e senza sapere (né dovendo sapere) che l'acquisizione viola i diritti di un terzo, acquista l'asset libero da pretese proprietarie altrui, anche se il suo dante causa non era legittimato a disporne. Questa regola, funzionalmente analoga a quella del "possesso vale titolo" per i beni mobili (art. 1153 c.c.), è indispensabile per garantire la sicurezza e la rapidità della circolazione in un ambiente digitale.
- **Dialogo con il Diritto Nazionale:** I Principi non mirano a sostituire integralmente il diritto nazionale, ma a dialogare con esso. Il Principio 3 distingue tra "Principles law" (la parte del diritto di uno Stato che implementa o è coerente con i Principi) e "other law" (tutto il resto del diritto di quello Stato). Quest'ultimo continua a regolare tutte le questioni non espressamente coperte dai Principi, come ad esempio la validità dei contratti, la disciplina della tutela del consumatore o il diritto di proprietà intellettuale.

Strumenti di Protezione: Un Dialogo tra Tecnologia e Diritto

La protezione dei beni digitali si articola su un duplice binario: da un lato, soluzioni tecnologiche di autotutela; dall'altro, strumenti giuridici tradizionali adattati al nuovo contesto.

Le Fortezze Tecnologiche – Modelli di Autotutela

Per mitigare i rischi intrinseci dell'ambiente digitale, quali il furto di chiavi private o gli attacchi hacker, esistono due approcci principali:

- **Wallet Multi-Firma (Multi-Sig):** Questa soluzione richiede un numero predefinito di firme crittografiche (M) da un gruppo di N co-firmatari per autorizzare una transazione. La sicurezza è garantita dalla condivisione delle responsabilità: un attaccante dovrebbe compromettere M chiavi private distinte per accedere ai

fondi. Tuttavia, i sistemi Multi-Sig sono spesso legati a specifiche blockchain e la visibilità on-chain delle firme multiple può compromettere la privacy e aumentare i costi di transazione (gas fees) a causa della maggiore complessità.

- **Multi-Party Computation (MPC):** Questa tecnologia rappresenta un'evoluzione del concetto Multi-Sig. Invece di utilizzare più chiavi private indipendenti, l'MPC frammenta una singola chiave privata in "shares" (frammenti crittografici) distribuite tra diverse parti o dispositivi. Queste shares vengono poi utilizzate per calcolare collettivamente una firma valida, senza mai ricostruire la chiave privata completa in un unico luogo o momento. Il processo di firma distribuita avviene off-chain, garantendo maggiore privacy (on-chain appare una firma singola standard), minori costi di transazione e una compatibilità fondamentale con diverse blockchain (cd. *blockchain agnosticism*).

La Cassaforte Giuridica – Il Trust per i Beni Digitali

Il trust, istituto di origine anglosassone ma ormai riconosciuto e utilizzato anche negli ordinamenti di civil law (in Italia tramite la ratifica della Convenzione dell'Aja del 1985), si rivela uno strumento straordinariamente versatile ed efficace per la gestione e la protezione dei beni digitali.

Il suo effetto principale è la **segregazione patrimoniale**. Il conferimento di un bene in trust (sia esso un immobile, una partecipazione o un portafoglio di cripto-attività) crea un patrimonio separato e autonomo. Questo patrimonio è intestato formalmente al trustee, ma è giuridicamente distinto sia dal patrimonio residuo del disponente sia dal patrimonio personale del trustee. Questo "scudo" giuridico rende i beni in trust insensibili alle vicende personali (debiti, fallimento, pretese dei creditori) sia del disponente che del trustee, garantendo una protezione robusta.

Nell'ambito della **pianificazione successoria**, il trust offre una soluzione elegante a uno dei problemi più critici dell'eredità digitale: la trasmissione sicura e controllata delle chiavi private e delle credenziali di accesso. La perdita di queste informazioni equivale alla perdita definitiva del bene. Attraverso il trust, il disponente può trasferire gli asset digitali al trustee, inserendo nell'atto istitutivo istruzioni precise e dettagliate su come custodire, gestire e, al momento della sua morte, distribuire tali asset (e le relative credenziali di accesso) ai beneficiari designati. Questo garantisce la continuità dell'accesso, previene la dispersione o la perdita del patrimonio digitale e permette una gestione flessibile e riservata, a differenza del testamento che è un atto pubblico.

La gestione di un trust di asset digitali, tuttavia, richiede competenze specifiche. Emerge la figura del **"trustee digitale"**: non basta più il tradizionale dovere fiduciario, ma è necessaria anche la capacità tecnica di custodire in sicurezza le chiavi private, interagire con le blockchain, gestire wallet e seguire le complesse istruzioni del

disponente. Questo sta portando alla nascita di trustee professionali e società fiduciarie specializzate nella gestione di patrimoni digitali.

La sfida della piena decentralizzazione – lo status giuridico delle DAO

Le Organizzazioni Autonome Decentralizzate (DAO) rappresentano una delle frontiere più radicali della governance digitale. Si tratta di forme organizzative native del web3, la cui struttura e le cui regole operative sono definite da smart contract eseguiti su una blockchain e la cui governance è affidata ai possessori di specifici token. Spesso, le DAO operano senza una struttura gerarchica tradizionale e, soprattutto, senza un'entità legale centrale di riferimento.

Questo le colloca in un pericoloso vuoto normativo. In assenza di una specifica forma giuridica, una DAO che svolge un'attività economica con terzi rischia di essere qualificata dalla giurisprudenza della maggior parte dei Paesi, Italia inclusa, come una **società di fatto** o un'associazione non riconosciuta. La conseguenza giuridica più grave di tale inquadramento è l'applicazione di un regime di **responsabilità personale, illimitata e solidale** di tutti i suoi membri per le obbligazioni assunte dall'organizzazione. Questo rischio rappresenta un enorme deterrente alla partecipazione, specialmente per gli investitori istituzionali e per chiunque abbia un patrimonio da proteggere.

Per ovviare a questo problema fondamentale, stanno emergendo soluzioni di **“legal wrapper”**, ovvero “involucri giuridici” che mirano a “vestire” la DAO con una forma giuridica tradizionale per conferirle personalità giuridica e, soprattutto, per limitare la responsabilità dei suoi membri. L'esempio più noto e discusso è la legge approvata nel 2021 dallo Stato del **Wyoming**, che permette a una DAO di registrarsi come una **Limited Liability Company (LLC)**, beneficiando così del regime di responsabilità limitata. Altri modelli emergenti utilizzano fondazioni o altre entità societarie in giurisdizioni considerate innovative e favorevoli, come la Svizzera o le Isole Marshall.

Il paradosso del legal wrapper per le DAO risiede nel fatto che, pur nascendo da ideali di decentralizzazione, esse necessitano di un’interfaccia legale per operare nel mondo reale (es. contratti, conti bancari, limitazione di responsabilità). Questa interfaccia reintroduce elementi di centralizzazione (giurisdizione, rappresentanti legali), contraddicendo l’obiettivo tecnologico iniziale. La sfida futura per le DAO sarà trovare un equilibrio tra decentralizzazione e le esigenze pratiche dell'interazione giuridico-economica.

Conclusioni: verso una governance integrata e multi-livello.

Il confronto tra *lex informatica* (codice auto-eseguibile) e la normativa statale in merito alla disciplina dei beni digitali rivela l'utopicità di una supremazia incondizionata del codice, al contempo evidenziando l'inefficacia di una regolamentazione statale disgiunta dalle innovazioni tecnologiche. La soluzione più plausibile si profila in una sintesi: la "lex cryptographica", in cui la legislazione statale stabilisce principi e limiti (ad esempio, la tutela dei consumatori, le normative antiriciclaggio), demandando alla tecnologia l'implementazione di tali direttive. Il Regolamento MiCAR ne costituisce un esempio paradigmico, definendo il "cosa" e il "perché" sul piano giuridico, ma lasciando il "come" alla sfera tecnologica.

La gestione dei beni digitali si articola su differenti livelli interconnessi: il **diritto pubblico** (ad esempio, MiCAR) disciplina il contesto macro-sistemico, assicurando stabilità e protezione. La **soft law** (come i Principi UNIDROIT) agevola la circolazione dei diritti privati a livello micro e transnazionale attraverso il concetto di "controllo". A livello individuale, la **tecnologia** (ad esempio, MPC) e il **diritto privato** (come il Trust) offrono soluzioni per la tutela e la pianificazione. Le **DAO** ridefiniscono il modello di governance societaria. Il futuro del diritto immateriale risiede nell'armonizzazione di tali livelli e non tanto in una unica, monolitica soluzione: siamo chiamati a costruire un ponte solido tra l'inarrestabile innovazione tecnologica e la necessaria tutela dei valori e degli interessi fondamentali che sono alla base di ogni ordinamento giuridico.