Beni digitali e proprietà. La qualificazione giuridica delle nuove entità immateriali

Week 3 – Regolazione e tutela dei beni digitali

Prof. Ermanno Calzolaio

Introduzione: dal “cosa” al come” governare

Come vengono regolati, protetti e governati questi asset immateriali?

Da un lato, assistiamo all'**affermazione della lex publica**, il diritto imperativo dei mercati, che trova la espressione nel Regolamento europeo **MiCAR**, il cui scopo è garantire **stabilità**, **trasparenza** e **protezione** degli investitori.

Dall'altro lato, emerge una **nuova lex privata**, una sorta di **lex mercatoria digitale**, incarnata dai Principi UNIDROIT. Questi ultimi mirano a forgiare un **linguaggio giuridico comune**, **flessibile** e **transnazionale**, per facilitare la circolazione dei diritti su tali beni. La **governance del digitale** si configura, quindi, come un sistema multi-livello che armonizza norme pubbliche, **principi di soft law**, strumenti privatistici tradizionali e forme di autotutela tecnologica.

Il Regolamento (UE) 2023/1114 (MiCAR)

Architettura e finalità del MiCAR

Il **Regolamento (UE) 2023/1114**, noto come MiCAR (**Markets in Crypto-Assets**), costituisce la prima e più organica iniziativa legislativa a livello globale per creare un quadro normativo armonizzato per le cripto-attività.
Base giuridica: **art. 114 TFUE**, segnalando l'ambizione di crare un mercato unico europeo per i servizi legati alle cripto-attività, introducendo un regime di ***passaporto europeo*** che consente agli operatori autorizzati in uno Stato membro di operare in tutta l'Unione.

Il Regolamento (UE) 2023/1114 (MiCAR)

Perimetro regolamentare del MiCAR

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

1. **Asset-Referenced Tokens (ART)**: Legati a un paniere di valute, commodity o altre cripto-attività.
2. **E-money Tokens (EMT)**: Ancorati al valore di una singola valuta ufficiale.
3. **"Altre Cripto-attività"**: Categoria residuale che include, ad esempio, gli utility token.

Restano esplicitamente fuori dal suo ambito di applicazione le cripto-attività uniche e non fungibili (NFT), a meno che la loro emissione in grandi serie non ne suggerisca la fungibilità. Aspetto cruciale, sono escluse anche le cripto-attività senza un emittente identificabile (come Bitcoin) e i servizi prestati in modo completamente decentralizzato, ovvero il cuore della Finanza Decentralizzata (DeFi).

Il Regolamento (UE) 2023/1114 (MiCAR)

La scelta pragmatica di regolare i “punti di contatto”.

La scelta del legislatore europeo di escludere la DeFi pura è eminentemente pragmatica.
Anziché tentare di regolare protocolli puramente decentralizzati, privi di un soggetto giuridico di riferimento, il MiCAR si concentra 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, ma crea un inevitabile **"donut hole" regolamentare**. La DeFi pura, dove i servizi sono forniti da smart contract autonomi, rimane formalmente non disciplinata. Il MiCAR regola le "rampe di accesso e di uscita" (exchange, custodi), ma non il nucleo decentralizzato dell'innovazione e del rischio.
A lungo termine, ciò potrebbe condurre a una biforcazione del mercato: da un lato, un settore regolamentato, integrato con la finanza tradizionale; dall'altro, un'area non regolamentata, più rischiosa ma potenzialmente più innovativa.

Il Regolamento (UE) 2023/1114 (MiCAR)

Un insieme di obblighi per emittenti e intermediari

Emittenti

- Devono essere costituiti come persone giuridiche.
- L'adempimento centrale è la redazione di un White Paper informativo, chiaro e non fuorviante, che fonda la loro responsabilità civile per informazioni scorrette.
- Per gli emittenti di ART ed EMT, gli obblighi sono più severi: necessitano di un'autorizzazione specifica e devono mantenere una riserva di attivi a copertura del 100% delle passività.

Intermediari (CASP)

- Devono ottenere un'autorizzazione per operare, beneficiando poi del "passaporto europeo".
- Sono soggetti a requisiti prudenziali (fondi propri o polizza assicurativa) e a rigorose regole di condotta a tutela dei clienti.
- In Italia, il decreto di adeguamento ha designato Banca d'Italia e Consob come autorità competenti.

Il Regolamento (UE) 2023/1114 (MiCAR)

Completare l’architettura di tutela

Il MiCAR istituisce un sistema di vigilanza a più livelli:

- A livello **nazionale**: Le autorità competenti (in Italia, Consob e Banca d'Italia) vigilano su emittenti e CASP.
- A livello **europeo**: L'Autorità Bancaria Europea (ABE) e l'Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA) coordinano, emanano standard tecnici e possono intervenire direttamente sui token "significativi".

L'innovazione più rilevante 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.

Una Lex Mercatoria digitale: i principi UNIDROIT

Armonizzare il diritto privato a livello globale

Parallelamente alla normativa pubblica, i **Principi UNIDROIT sugli Asset Digitali (maggio 2023)** si propongono come strumento di soft law a carattere transnazionale.

Natura e Funzione:

- Non sono direttamente vincolanti, ma agiscono come raccomandazioni per legislatori e operatori.
- Perseguono un approccio di neutralità tecnologica e giurisdizionale.
- L'obiettivo è creare un impianto concettuale duttile per aumentare la certezza del diritto e l'efficienza delle transazioni transfrontaliere, riducendo i costi e facilitando il commercio globale.

Una Lex Mercatoria digitale: i principi UNIDROIT

Dal dominio al “controllo”

Il cuore dogmatico dei Principi UNIDROIT risiede nell'elaborazione della nozione di “**controllo**” (**Principio 6**), quale alternativa al concetto di “**proprietà**”. Il controllo non è un diritto astratto, ma una situazione di fatto, funzionale e tecnicamente verificabile.
Una persona ha il controllo di un asset digitale se ha la capacità fattuale ed esclusiva di:

1. Ottenere sostanzialmente tutti i benefici dall'asset (**controllo positivo**).
2. Impedire ad altri di ottenerli (**controllo negativo**).
3. **Trasferire tale capacità ad altri**.

Questa scelta strategica sposta il focus dal titolo giuridico (spesso divisivo tra ordinamenti di civil e common law) alla **relazione funzionale con l’asset**. Il "controllo" diventa così il **corrispettivo funzionale del “possesso”** per i beni materiali, accertabile da qualsiasi giudice sulla base di prove tecniche.

Una Lex Mercatoria digitale: i principi UNIDROIT

Regole fondamentali per la fiducia e la circolazione transfrontaliera

Basandosi sul concetto di controllo, i Principi stabiliscono regole fondamentali per un **mercato prevedibile, certo e sicuro**:

- **Tutela nella custodia** (Principio 13): Viene sancito il principio di segregazione patrimoniale. Gli asset digitali detenuti da un custode per un cliente non fanno parte della massa fallimentare del custode e non sono aggredibili dai suoi creditori.
- **Acquisto in buona fede** (Principio 8): Viene introdotta una regola di innocent acquisition. Chi acquista il controllo di un asset a titolo oneroso e in buona fede, ne acquista la titolarità libera da pretese altrui, anche se il dante causa non era legittimato. È una regola funzionalmente analoga al "possesso vale titolo" (art. 1153 c.c.), indispensabile per la sicurezza dei traffici.

Modelli di autotutela

Un dialogo tra tecnologia e diritto

La protezione dei beni digitali si articola su un **duplice binario**. Prima di esaminare gli strumenti giuridici, analizziamo le soluzioni tecnologiche di autotutela.

- **Wallet Multi-Firma (Multi-Sig)**: Richiede M-firme su N-totali per autorizzare una transazione. La sicurezza è distribuita, ma la visibilità on-chain può compromettere la privacy e aumentare i costi di transazione.
- **Multi-Party Computation (MPC)**: Rappresenta un'evoluzione. Una singola chiave privata viene frammentata in "shares" distribuite tra più parti. La firma viene calcolata collettivamente senza mai ricostruire la chiave completa. Questo processo, avvenendo off-chain, garantisce maggiore privacy, minori costi ed è compatibile con diverse blockchain (blockchain agnosticism).

Crisi della materialità e beni digitali

Caratteristica	Wallet Multi-Firma (Multi-Sig)	Wallet Multi-Party Computation (MPC)
Principio di Sicurezza	Condivisione della responsabilità: M-di-N chiavi private indipendenti.	Frammentazione della conoscenza: una singola chiave privata è divisa in "shares" che non vengono mai assemblate.
Punto di Fallimento	Nessun singolo punto di fallimento (richiede la compromissione di M chiavi).	Nessun singolo punto di fallimento (richiede la compromissione di una soglia di shares).
Blockchain "agnosticism"	Limitato. Tipicamente specifico per ogni blockchain (es. Bitcoin, Ethereum hanno implementazioni diverse).	Elevato. Agnostico rispetto alla blockchain, supporta qualsiasi catena che usi algoritmi di firma standard (es. ECDSA).
Privacy On-Chain	Bassa. Le firme multiple e gli indirizzi dei firmatari sono registrati on-chain.	Alta. La firma finale appare on-chain come una firma singola standard. Il processo di firma collettiva è off-chain.
Costi di Transazione (Gas)	Più alti. Le transazioni Multi-Sig sono più complesse e richiedono più dati on-chain.	Più bassi. La transazione finale è standard, con costi inferiori.
Flessibilità Operativa	Rigida. Modificare il numero di firmatari o le soglie richiede la creazione di un nuovo wallet.	Flessibile. Le soglie e i partecipanti possono essere modificati dinamicamente senza cambiare l'indirizzo del wallet.
Velocità di Transazione	Potenzialmente più lenta a causa della complessità on-chain.	Più veloce, poiché la computazione complessa avviene off-chain.

Modelli di autotutela

Adattare strumenti tradizionali a scopi innovativi: il trust

Il trust si rivela uno strumento straordinariamente efficace per la gestione dei beni digitali.

- **Effetto principale → segregazione patrimoniale**. Il bene conferito in trust costituisce un patrimonio separato e autonomo, intestato al trustee ma insensibile alle vicende personali (debiti, fallimento) sia del disponente che del trustee stesso.
- **Applicazione nella pianificazione successoria**: Il trust offre una soluzione al problema della trasmissione delle chiavi private. Il disponente può trasferire gli asset al *trustee* con istruzioni precise sulla loro custodia, gestione e distribuzione ai beneficiari, garantendo continuità e riservatezza.
- **Nasce la figura del "Trustee Digitale"**: Un professionista che unisce al dovere fiduciario la competenza tecnica per gestire in sicurezza asset su blockchain.

Modelli di autotutela

Lo status giuridico delle DAO: decentralizzazione vs. personalità

Le **Organizzazioni Autonome Decentralizzate (DAO)** rappresentano una frontiera radicale. Sono organizzazioni le cui regole sono incise in smart contract e la cui governance è affidata ai possessori di token, spesso senza un'entità legale di riferimento.
Questo le colloca in un **pericoloso vuoto normativo**. In assenza di una forma giuridica, una DAO rischia di essere qualificata come società di fatto o associazione не riconosciuta. La conseguenza più grave è la responsabilità personale, illimitata e solidale di tutti i suoi membri.
Per ovviare a questo rischio, emergono soluzioni di **“legal wrapper”**: **"involucri giuridici"** (come la LLC del Wyoming) che "vestono" la DAO con una forma legale tradizionale per conferirle personalità giuridica e, soprattutto, limitare la responsabilità dei membri.

Conclusioni

La sintesi tra codice e legge?

Il confronto tra la lex informatica (il codice) e la normativa statale dimostra l'utopia di una supremazia assoluta del codice, ma anche l'inefficacia di una legge avulsa dalla tecnologia. La soluzione si profila in una sintesi: la "lex cryptographica", dove la legge statale fissa principi e limiti, mentre la tecnologia ne cura l'implementazione.
La governance dei beni digitali si articola su livelli interconnessi:

- **Hard Law (MiCAR)**: Assicura stabilità e protezione a livello macro-sistemico.
- **Soft Law (UNIDROIT)**: Facilita la circolazione transnazionale dei diritti privati.
- **Tecnologia (MPC) e diritto privato (trust)**: Offrono soluzioni di tutela a livello individuale.
- **Nuovi modelli (DAO)**: Ridefiniscono la governance organizzativa.

Il **futuro del diritto dei beni digitali** non risiede in una soluzione monolitica, ma nell'armonizzazione di questi livelli, costruendo un ponte solido tra l'inarrestabile innovazione tecnologica e la necessaria tutela dei valori fondamentali dell'ordinamento giuridico.