FORNARI E ASSOCIATI

STUDIO LEGALE

# FOCUS

## NUOVE FRONTIERE REGOLATORIE EUROPEE

### Il filo conduttore tra crypto-attività, cybersicurezza, finanza e sanità

fornarieassociati.com

Milano • Roma • Bari

Febbraio 2025

# NUOVE FRONTIERE REGOLATORIE EUROPEE: IL FILO CONDUTTORE TRA CRYPTO-ATTIVITÀ, CYBERSICUREZZA, FINANZA E SANITÀ

## Indice



## 1. Introduzione

La rapida evoluzione tecnologica degli ultimi anni ha portato alla nascita di nuove sfide regolatorie in ambiti cruciali come quello delle crypto-attività, della cybersicurezza, finanziario e sanitario. Un filo conduttore lega questi settori: la necessità di una regolamentazione uniforme, capace di garantire una protezione adeguata dei cittadini, delle imprese e degli investitori, affrontando in modo sinergico le sfide legate all'innovazione tecnologica, alla sicurezza e alla trasparenza.

In particolare, il Regolamento MiCA sulle crypto-attività, la Direttiva NIS 2 sulla cybersicurezza, il Digital Operational Resilience Act nel settore finanziario e il Sunshine Act in ambito sanitario rappresentano risposte normative alle nuove vulnerabilità e ai rischi emergenti.

Il presente Focus si pone come obiettivo quello di approfondire le principali novità introdotte dai quattro provvedimenti (MiCA, NIS 2, DORA e Sunshine Act), per facilitare gli operatori dei rispettivi settori nell'adeguamento alle nuove disposizioni normative.

## 2. Crypto-attività: il Regolamento MiCA

Con il Regolamento (UE) 2023/1114 del 31 maggio 2023 (d'ora in avanti, "**Regolamento MiCA**"), l'Unione Europea è intervenuta nell'intricato contesto delle cripto-attività predisponendo un quadro normativo armonizzato e promuovendo un ecosistema digitale competitivo. In sintesi, il Regolamento MiCA ("*Markets in Crypto-Assets*") ha delineato per la prima volta un *framework* organico che disciplina l'emissione, l'offerta e la negoziazione di specifiche categorie di cripto-attività, mirando a conciliare l'innovazione tecnologica con la protezione degli investitori e la stabilità finanziaria. L'obiettivo è quindi quello di favorire lo sviluppo e la competitività del settore delle cripto-attività in Europa, un ambito già parzialmente regolato in specifici settori, come quello antiriciclaggio e fiscale.

Cripto-attività: una *overview*

Le cripto-attività sono rappresentazioni digitali di valore o diritti. Possono essere impiegate come mezzo di pagamento (c.d. criptovalute), per accedere a beni o servizi (c.d. *utility token*) o anche a fini di investimento.

Possono essere trasferite e archiviate elettronicamente tramite la tecnologia a registro distribuito (DLT), vale a dire una tecnologia che consente l'archiviazione, l'aggiornamento e la convalida decentrati di dati criptati.[1]

L'evidenza dimostra che le cripto-attività sono in grado di semplificare i processi di raccolta di capitali e di rafforzare la concorrenza, offrendo – specialmente alle PMI – un approccio innovativo al finanziamento. Apportano significativi vantaggi anche ai piccoli investitori, soprattutto a livello transfrontaliero, riducendo la necessità dell'intervento di intermediari finanziari tradizionali.

D'altra parte, è proprio l'assenza di intermediari che non permette l'innesto di punti di controllo funzionali a rilevare indirizzi ed identità.

Ancora, appare utile evidenziare come le cripto-attività si caratterizzino per l'assenza di controparti centrali e per la decentralizzazione della gestione delle transazioni, fattori che rendono particolarmente difficile una eventuale risposta normativa tempestiva ed efficace.

Il quadro normativo prima del Regolamento MiCA

Prima dell'entrata in vigore del Regolamento MiCA, il quadro normativo europeo in materia di cripto-attività era caratterizzato da una notevole frammentazione. Se da un lato alcune cripto-attività, in particolare quelle qualificabili come "strumenti finanziari" ai sensi della Direttiva 2014/65/UE del Parlamento Europeo e del Consiglio, erano già disciplinate da norme chiare e complete, molte altre non godevano di una regolamentazione specifica.

Questa lacuna esponeva i detentori di cripto-attività a rischi considerevoli, in particolare in ambiti non protetti dalle normative sulla tutela dei consumatori. Inoltre, comportava rischi significativi per l'integrità del mercato – tra cui abusi di mercato e crimini finanziari – e precludeva alle aziende l'opportunità di crescere sotto il profilo dell'innovazione digitale.

Peraltro, il protrarsi di questo scenario avrebbe probabilmente portato a una frammentazione delle discipline nazionali, alterando la concorrenza nel mercato unico e ostacolando l'espansione transfrontaliera dei fornitori di servizi legati alle cripto-attività.

I punti chiave

Il MiCA si è posto la realizzazione di diversi obiettivi chiave, quali ad esempio:

1. **sostenere l'innovazione e promuovere la concorrenza leale**, permettendo ai prestatori di servizi la crescita del mercato senza ostacoli normativi fuori misura;
2. **proteggere gli investitori e la stabilità dei mercati**. A tal fine, il Regolamento introduce misure specifiche che garantiscono un elevato livello di tutela per i detentori al dettaglio e preservano l'integrità dei mercati delle cripto-attività, inclusi requisiti di trasparenza e di informativa per prevenire frodi e pratiche scorrette;
3. **facilitare l'accesso ai servizi bancari per i prestatori di servizi per le cripto-**

[1] Un esempio di DLT sono le *blockchain*: qui i dati registrati sono aggiunti in "blocchi", che compongono una "catena" indistruttibile.

**attività**, incentivando una maggiore integrazione tra i servizi finanziari tradizionali e quelli basati su cripto-attività, e permettendo alle imprese di operare con maggiore agilità nell'ambito del mercato unico europeo;

4. **stabilire obblighi di rendicontazione relativi agli effetti ambientali delle cripto-attività**, per aumentare la consapevolezza sull'impatto ecologico. A tal fine, sono coinvolte l'Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA) e l'Autorità Bancaria Europea (EBA), che si occuperanno di sviluppare norme tecniche dettagliate riguardanti la rendicontazione ambientale e i principali indicatori energetici.

## 3. Cybersicurezza: la Direttiva NIS 2

Nell'attuale contesto digitale, la Direttiva NIS 2 istituisce un quadro giuridico armonizzato in tutta l'UE per sostenere la cybersicurezza in 18 settori critici.

La sicurezza informatica riguarda la protezione delle reti e dei sistemi informativi (NIS), degli utenti e di tutti coloro che possono subire incidenti e minacce informatiche. Per fronteggiare la crescente esposizione dell'Europa alle minacce cibernetiche e per garantire un'applicazione efficace a livello transfrontaliero, la Direttiva 2022/2555, conosciuta anche come "**NIS 2**", ha sostituito la precedente Direttiva 2016/1148 o NIS 1. Rispetto a quest'ultima, la Direttiva NIS 2 innalza il livello di attenzione dell'UE sulla cybersicurezza, ampliando l'ambito di applicazione, introducendo norme più precise e rafforzando gli strumenti di vigilanza.

### Prima e dopo la Direttiva NIS 2

Con la Direttiva NIS 1, l'Unione Europea ha promosso per la prima volta una normativa volta a rafforzare la sicurezza delle reti e dei sistemi informativi. All'esito dell'iter di revisione della Direttiva NIS 1 (avviato dalla Commissione nel dicembre 2020), è stata poi adottata la Direttiva NIS 2, entrata in vigore nel gennaio 2023. Gli Stati membri avevano tempo fino al 17 ottobre 2024 per recepirla nel diritto nazionale, con la conseguente abrogazione definitiva di NIS 1 a partire dal 18 ottobre 2024.

In seguito a tale scadenza, la Commissione ha avviato procedure di infrazione, inviando lettere di costituzione in mora a 23 Stati membri che non avevano pienamente recepito la Direttiva NIS 2 entro il termine stabilito. Gli Stati membri devono quindi rispondere e portare a termine il processo di recepimento della Direttiva.

### I punti chiave

La Direttiva impone agli Stati membri di rafforzare le capacità in materia di cybersicurezza introducendo misure di gestione dei rischi e obblighi di segnalazione e stabilendo norme per la cooperazione, la condivisione delle informazioni e la vigilanza. Recepita in Italia con Decreto Legislativo n. 138/2024, la NIS 2 interviene su diversi aspetti:

1. **Strategia nazionale in cybersicurezza**: ogni Stato membro è tenuto ad adottare una strategia nazionale in materia di cybersicurezza e a mantenere aggiornato un elenco di operatori di servizi essenziali, assicurandosi che tali soggetti rispettino i requisiti della Direttiva;
2. **Ambito di applicazione**: oltre ai settori già inclusi nella Direttiva NIS 1 – quali

quello energetico, dei trasporti, sanitario, finanziario, relativo alla gestione delle risorse idriche e delle infrastrutture digitali – la NIS 2 identifica (i) nuovi settori sottoposti agli obblighi di cybersicurezza, dividendoli in "altamente critici" e "critici", e (ii) nuovi soggetti, classificati in "essenziali" e "importanti", in funzione della rilevanza per il settore o il tipo di servizi che forniscono. I soggetti di medie e grandi dimensioni dei settori critici devono adottare misure adeguate per la gestione dei rischi informatici e notificare gli incidenti significativi alle autorità nazionali competenti (si tratta di incidenti che potrebbero causare interruzioni o danni di rilevante entità);

3. **Vigilanza**: sono incluse misure di vigilanza più rigorose e un sistema sanzionatorio più severo, con l'obiettivo di rafforzare la fiducia reciproca e le capacità di cybersicurezza in tutta l'Unione Europea;
4. **Responsabilità della dirigenza**: è prevista la responsabilità dell'alta dirigenza per il mancato rispetto delle misure di gestione dei rischi informatici, così incentivando gli organi di *corporate governance* a partecipare attivamente e costantemente al processo decisionale sulla cybersicurezza;
5. **Reti di intervento per la sicurezza informatica**: è istituita una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), finalizzata alla condivisione delle informazioni sulle minacce informatiche e alla gestione degli incidenti. Inoltre, la Direttiva istituisce la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), a garanzia del regolare scambio di informazioni tra gli Stati membri e le istituzioni dell'UE in caso, appunto, di incidenti e crisi su vasta scala.

## 4. Finanza: il Digital Operational Resilience Act (DORA)

Il Regolamento (UE) 2022/2554 (d'ora in avanti "Digital Operational Resilience Act", comunemente noto come "**DORA**"), entrato in vigore il 16 gennaio 2023 e operativo dal 17 gennaio 2025, affronta una lacuna critica nella regolamentazione finanziaria dell'UE: il rischio ICT nel settore finanziario.

Se è infatti appurato che le nuove tecnologie digitali rappresentano un'importante leva per incrementare l'efficienza dei sistemi finanziari, è proprio questo legame a rendere le entità finanziarie vulnerabili ad attacchi informatici o attività illecite. Se non gestiti correttamente, i rischi ICT possono causare interruzioni dei servizi finanziari, con effetti a catena su altre aziende, settori e persino sul resto dell'economia. In questo contesto, la resilienza operativa digitale del settore finanziario assume primaria importanza.

Prima del DORA, gli istituti finanziari gestivano i rischi operativi principalmente attraverso l'allocazione di capitale per coprire eventuali perdite. Sul punto, invece, DORA riconosce che gli incidenti ICT possono minacciare la stabilità dell'intero sistema finanziario, anche quando viene assegnato un capitale "adeguato" alle categorie di rischio tradizionali.

Il Regolamento si applica a tutte le istituzioni finanziarie dell'UE, ricomprendendo sia le entità "tradizionali" quali banche, società di investimento e istituti di credito, sia quelle "non tradizionali" come fornitori di asset legati a criptovalute e piattaforme di *crowdfunding*.

Il suo obiettivo è pertanto quello di rafforzare la sicurezza informatica degli enti finanziari e garantire che l'intero settore sia resiliente in caso di grave interruzione operativa.

I punti chiave

1. **Gestione del rischio ICT**: il Regolamento DORA attribuisce la responsabilità della gestione dei rischi ICT all'organo amministrativo. A tal fine, è necessario mappare i sistemi ICT, identificare le minacce informatiche e documentare le misure preventive adottate per ridurre i rischi individuati. Inoltre, devono essere definiti piani di continuità operativa e *disaster recovery* considerando vari scenari di rischio, come guasti nei servizi ICT, calamità naturali e attacchi *cyber*;
2. **Gestione del rischio di terze parti**: una nota caratteristica del Regolamento DORA è l'estensione della sua applicabilità ai fornitori ICT che servono il settore finanziario. Pertanto, gli enti finanziari non potranno stipulare contratti con fornitori ICT non conformi al Regolamento DORA e saranno tenuti a mappare le proprie dipendenze ICT di terze parti;
3. **Test di resilienza operativa digitale**: le entità finanziarie sono tenute ad eseguire test periodici sui propri sistemi ICT per valutare l'efficacia delle misure di protezione e individuare eventuali vulnerabilità;
4. **Reportistica in caso di incidenti ICT**: a seconda della gravità dell'incidente, le istituzioni finanziarie potrebbero essere obbligate a segnalare l'accaduto sia alle autorità competenti, sia ai clienti e ai partner coinvolti;
5. **Condivisione delle informazioni**: le entità finanziarie devono implementare processi di apprendimento basati sugli incidenti ICT, sia interni che esterni. A tal fine, il Regolamento DORA incoraggia la condivisione di informazioni relative alla *threat intelligence* tra le organizzazioni.

## 5. Sanità: il Sunshine Act

Sulla base dei modelli già sperimentati all'estero (in particolare quello francese e quello statunitense), l'Italia ha introdotto, con Legge n. 62 del 31 maggio 2022, una normativa volta a garantire la trasparenza nei rapporti tra le imprese e i soggetti operanti nel settore sanitario, il c.d. "**Sunshine Act** ".

Sebbene già con il Codice della trasparenza (D. Lgs. n. 33/2013) erano stati riorganizzati e potenziati gli obblighi di trasparenza in capo alle pubbliche amministrazioni, inducendo le aziende produttrici di prodotti bio-medicali ad adottare, tramite i codici deontologici di categoria, obblighi di trasparenza per le imprese associate, con il Sunshine Act, gli obblighi di trasparenza saranno applicabili uniformemente a tutte le aziende del settore, indipendentemente dall'appartenenza a una specifica associazione di categoria.

I punti-chiave

1. **Obblighi di trasparenza**: il Sunshine Act prevede che le aziende produttrici di

beni e servizi medicali rendano pubbliche tutte le erogazioni di denaro, relative a beni, servizi o altri benefici a favore di (i) soggetti operanti nel settore sanitario e (ii) organizzazioni sanitarie. Nel primo caso, il valore per singola erogazione deve superare i 100 euro, o l'importo complessivo annuo deve eccedere i 1.000 euro; nel secondo caso, la somma per singola erogazione deve essere maggiore di 1.000 euro o il totale annuo deve superare i 2.500 euro (art. 3, comma 1). Devono essere divulgati anche i vantaggi diretti o indiretti a favore di tali soggetti, come conferenze, eventi formativi e comitati scientifici (art. 3, comma 2).

Inoltre, ogni anno, le imprese produttrici strutturate come società devono trasmettere al Ministero della Salute i dati identificativi delle persone fisiche che possiedono azioni, quote del capitale sociale o obbligazioni emesse dall'impresa registrate nell'anno precedente, oppure delle persone fisiche che, nell'anno precedente, abbiano ricevuto compensi dall'impresa per la concessione di licenze di utilizzazione economica di diritti di proprietà industriale o intellettuale (art. 4);

2. **Il registro pubblico elettronico "Sanità trasparente"**: le comunicazioni di cui al punto precedente devono essere effettuate tramite il registro pubblico elettronico "Sanità trasparente", che è attualmente in fase di sviluppo;
3. **Sanzioni**: il Sunshine Act stabilisce uno specifico quadro sanzionatorio in caso di omissioni o di false comunicazioni. Ad esempio, nel caso di omessa comunicazione di erogazioni, convenzioni o accordi, l'impresa produttrice subirà una sanzione pari a 1.000 euro, aumentata di un importo pari a venti volte l'ammontare dell'erogazione non dichiarata. Invece, la mancata comunicazione di partecipazioni azionarie, titoli obbligazionari, proventi derivanti da diritti di proprietà industriale o intellettuale è punita con una sanzione da 5.000 a 50.000 euro.

## 6. Conclusioni

L'implementazione di nuove leggi nei settori delle crypto-attività, della cybersicurezza, della finanza e della sanità risponde alla necessità di fronteggiare le attuali sfide tecnologiche e i rischi emergenti.

Il Regolamento MiCA offre finalmente un quadro normativo chiaro per le crypto-attività, mentre la Direttiva NIS 2 e il Digital Operational Resilience Act (DORA) rafforzano la protezione contro le minacce informatiche e i rischi operativi nel settore finanziario. Sulla stessa linea, il Sunshine Act garantisce maggiore trasparenza nei rapporti tra le imprese e i soggetti del settore sanitario, migliorando la fiducia nel pubblico.

La convergenza di questi interventi normativi evidenzia la necessità di un approccio integrato alla regolamentazione, in grado di affrontare le vulnerabilità derivanti dalla digitalizzazione e di promuovere un ambiente sicuro, trasparente e competitivo.

La principale sfida per gli operatori rimane quella di adattarsi con prontezza ad un contesto in continua evoluzione.

# CONTACTS

**Giuseppe Fornari**
Founding Partner
g.fornari@fornarieassociati.com

**Pasquale Grella**
Of Counsel
p.grella@fornarieassociati.com

**Laura Beretta**
Trainee
l.beretta@fornarieassociati.com

**Milano**
Via Chiossetto 18
T: +39 0254122206
E: milano@fornarieassociati.com

**Roma**
Piazza Adriana 5
T: +39 0622201000
E: roma@fornarieassociati.com

**Bari**
Via Principe Amedeo 25
T: +39 080 918 4280
E: bari@fornarieassociati.com



**Fornari e Associati**

www.fornarieassociati.com