Università Europea di Roma

Co-funded by the European Union

JEAN MONNET CHAIR IN DIGITAL TRANSFORMATION AND AI POLICY

AI AND DECENTRALIZED FINANCE

Course Market Law and Regulation a.y. 2024-2025

Course convenor: Professor Valeria Falce (Valeria.Falce@unier.it)

.

Università Europea di Roma

Co-funded by the European Union

Introduction
Open Banking (and Open Finance): Challenges, Opportunities, and Regulatory Risks

An analysis of international legislative initiatives that are reshaping the banking and financial landscape through mandatory consumer data sharing

Introduction

- This presentation provides a comprehensive legal analysis of the transition from *Open Banking* to *Open Finance*, framed within the European Union's digital finance regulatory agenda;
- Key instruments to be examined include the Payment Services Directive 2 (PSD2, Directive (EU) 2015/2366), the proposed PSD3 package (COM/2023/366 final), the Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554), the Markets in Crypto-Assets Regulation (MiCA, Regulation (EU) 2023/1114), and the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), often referred to as the "Genius Act.";
- These frameworks reshape financial services by imposing obligations on banks, fintech companies, and crypto-asset issuers while creating new rights for consumers;
- The overarching objective is to identify challenges, assess risks, and propose policy solutions that balance innovation and financial stability.

Co-funded by the European Union

Key Legislative Initiatives

The international landscape is characterized by important regulatory developments that promote Open Banking through mandatory measures:

- Proposal for “Personal Financial Data Rights” by the US CFPB;
- Revision of the European PSD2 Directive;
- Introduction of Open Finance (FIDA) in the EU

These developments mark a significant transition: the United States, traditionally oriented toward a market-driven model, is moving closer to the European regulatory approach.

Università Europea di Roma

Co-funded by the European Union

Why the Regulatory Intervention Is Necessary

Open Banking is part of the recent wave of regulatory measures aimed at promoting data sharing and giving individuals greater control over their data in order to stimulate competition and innovation in financial markets.

Protecting Consumers

Ensuring consumers have effective control over their data and the opportunity to benefit from innovative and more competitive services provided by FinTech companies.

Promoting Competition

Reducing switching costs and avoiding the blocking of personal data, strengthening consumers' negotiating position vis-à-vis banks.

Fostering Innovation

Promoting financial inclusion through FinTech products and services that use large volumes of data, including non-financial data.

> “The economic logic underlying Open Banking is essentially competitive, as illustrated by the experience of the United Kingdom, where the regulatory remedy was conceived by an antitrust authority.”

Why Open Access Matters

- Open access is not merely a technological feature, but a legal mandate designed to enhance competition, consumer rights, and innovation. Under PSD2, banks must share customer account data with licensed third-party providers, subject to consumer consent.
- This strengthens the right to data portability under Article 20 GDPR and disrupts the traditional monopoly of banks over financial data. The policy rationale is to stimulate market entry by fintech firms, foster innovation, and extend financial services to underserved populations.
- Yet, open access also brings legal risks: liability for breaches, cybersecurity vulnerabilities, and potential consumer exploitation through deceptive consent mechanisms. These concerns necessitate a careful regulatory balance between openness and safeguards.

Università Europea di Roma

Co-funded by the European Union

Toward the Open Finance

The evolution of Open Banking towards Open Finance represents a fundamental step in Europe's "digital decade," with the aim of boosting the European financial data market through the new "Financial Data Access and Payments Package" regulatory framework.

Defining Open Banking, Open Finance, Open Access

Co-funded by the European Union

- Open Banking, anchored in PSD2, requires financial institutions to provide secure API access to customer payment account data and enable third-party payment initiation.
- Open Finance, currently being designed through PSD3, expands this framework to cover broader financial products, including investments, pensions, mortgages, and insurance.
- Open Access is the underlying principle, ensuring that consumers—not institutions—control their data.
- In the EU legal system, this principle aligns financial regulation with broader objectives of the Digital Single Market and the European Data Strategy, which promote cross-sector data sharing and interoperability.

The Shift to Consumer Data Control: Innovation vs Risk

Co-funded by the European Union

- The EU's regulatory framework reflects a decisive shift of control from banks to consumers. Under GDPR, individuals hold the right to data portability, which PSD2 translated into sector-specific obligations for banks. In practice, this means a customer can instruct a licensed fintech to access their account data, obliging the bank to comply.
- This marks a profound legal change: consumers are no longer passive users of banking services but active participants with enforceable rights. The shift also raises questions about liability allocation between banks and third-party providers, especially when breaches occur. EU law responds with layered compliance obligations, including Strong Customer Authentication under PSD2 and supervisory oversight of fintech actors.
- The EU legislator consistently seeks to balance innovation with financial stability. PSD2 facilitates innovation but mitigates risks through authentication and fraud-prevention measures. MiCA legitimises crypto-assets while imposing prudential and governance obligations on issuers of stablecoins, which are considered systemic if widely adopted. The EU AI Act embraces artificial intelligence in finance but classifies credit scoring and fraud detection as "high-risk systems" (Articles 6–9 AI Act), subjecting them to rigorous compliance obligations.

The Centrifugal Forces of the Financial Sector

Vertical Disintegration

Resizing of the traditional role of banks as the "first point of contact" and expansion of digital platforms that assume the role of "re-intermediaries" in the market.

- Loss of centrality of traditional banks
- Emergence of new digital intermediaries
- Integration of financial and non-financial services

Horizontal Disintegration

Increasing use of hard information, including non-financial data, which enables technologies such as artificial intelligence and machine learning.

- More comprehensive and structured information
- Ease of data sharing
- Acceleration of new innovative services

Financial Data Access and Payme Package

Co-funded by the European Union

The European regulatory response is structured around three complementary legislative instruments that operate on separate but interconnected levels.

Payment Services Regulation (PSR)

Regulation on payment services in the internal market - comprehensive regulation of payment service providers

Payment Services Directive 3 (PSD3)

Payment Services and Electronic Money Directive - rules on authorization and supervision of institutions

Financial Data Access (FiDA)

Regulation on access to financial data - data sharing regime in the European Union

VINCE IN BONO MALUM
Università Europea di Roma

PSD3: Supervision and Authorisation

Main Innovations

- Single authorization for PSPs and IMELs that do not collect deposits
- Mandatory liquidation plan in the event of insolvency
- Three-month deadline for the authorization process
- Update of capital requirements for inflation
- Possibility of custody at the central bank

Governance e Controls

Careful assessment of the governance plan with verification of the adequacy of internal corporate governance mechanisms, following the principle of proportionality.

The EBA shall develop draft technical standards to specify the information required and the common assessment criteria for the granting of authorization.

PSR: Transparency and Open Banking

01

Mandatory Dedicated Interfaces

Account servicing payment service providers must have a dedicated interface for data access, with a permanent backup interface for TPPs.

02

Management Panels

Tools integrated into the user interface to monitor and manage authorizations issued for account information services or payment order execution.

03

Enhanced Responsibilities

New provisions for unauthorized transactions, fraud, and the responsibilities of technical service providers in strong customer authentication.

FiDA: Open Finance Architecture

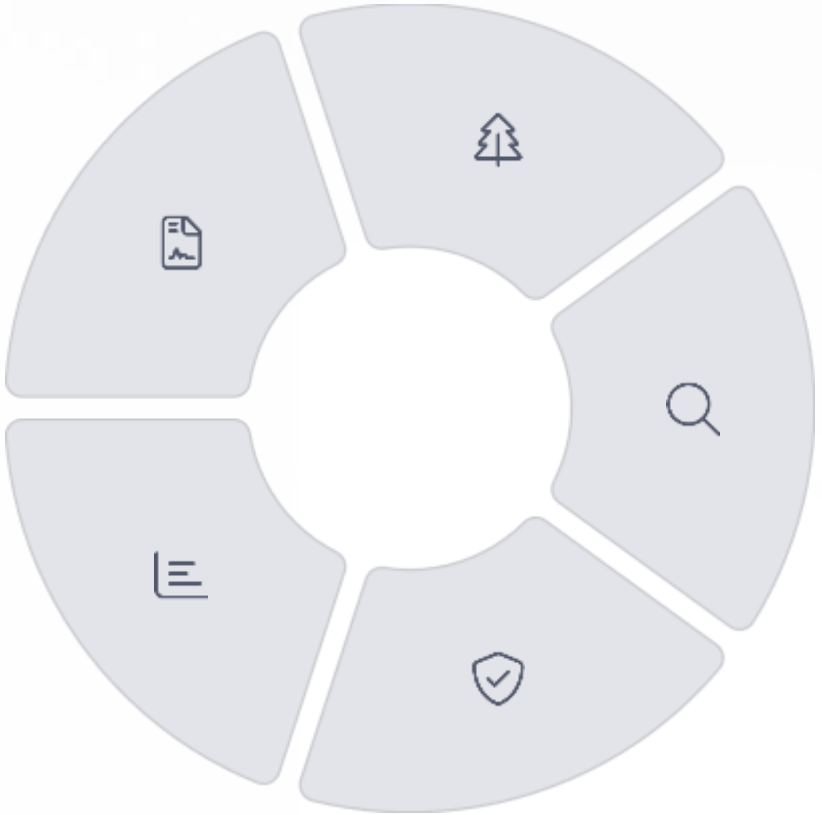
The FiDA regulation introduces a comprehensive framework for accessing and using financial data, creating the role of Financial Information Service Provider (FISP).

Credit Agreement

Data on mortgages, loans, and accounts (excluding payment accounts) to improve the overview of customer deposits.

Credit Assessment

Data for assessing the creditworthiness of companies, collected during loan application or rating procedures.



Investments

Data on savings, investments in financial instruments, insurance products, crypto-assets, and real estate.

Pension Rights

Data on corporate, professional, and individual pension products to develop pension tracking tools.

Non-Life Insurance

Insurance products (excluding health insurance) offering personalized protection for homes, vehicles, and other assets.

Università Europea di Roma

Co-funded by the European Union

Obligations and Liabilities within the FiDA

Università Europea di Roma

Co-funded by the European Union

Data Owners

- Free provision of data to customers
- Continuous, real-time sharing
- Possibility to request compensation from users
- Use of standardized formats
- Communication via secure channels

Data Users

- Mandatory prior authorization
- Exclusive use for authorized purposes
- Appropriate technical and organizational measures
- Adequate level of security
- Compliance with the principle of minimization

The entire data sharing system is based primarily on the consent given by the customer, assuming that consumers are prudent, responsible, and aware.

Management Panels and Sharing Systems

Management Panel

Front-end interface developed by the data owner to enable the customer to monitor and manage the permissions granted to data users.

- Overview of pending authorizations
- Possibility of revocation and restoration
- Register of authorizations for two years

Sharing Systems

Standardized frameworks governing access to specific data sets and internal governance rules for interaction between financial institutions.

- Equal and representative governance
- Access under the same conditions for everyone
- Transparent compensation model

Financial Information Service Providers (FISP)

Request for Authorisation

Detailed description of technical and organizational structures, legal status, responsible administrators with integrity and experience requirements.

Capital Requirements

Minimum capital of €50,000 or professional liability insurance or similar guarantee for liability coverage.

EBA Registration

Registration in the appropriate register managed by the EBA. For non-EU FISPs, a responsible European representative is required.

Continuous Supervision

Possibility of revocation for non-use for more than 12 months, false statements, or risks to consumer protection and data security.

Co-funded by the European Union

Università Europea di Roma

Co-funded by the European Union

Towards a New Legal Order for the Market

Discontinuities in information and communication confirm the profound transformation of the financial industry, contributing to the emergence of a new legal order in the market.

Standardization and Interoperability

The opening up of communication must be accompanied by data standardization and interoperability between infrastructures to enable effective portability of data and services.

Balancing Interests

Balancing economic, security, and privacy aspects, applying the principle of proportionality without excessively interfering with technological potential.

Regulatory Support

Using digital technologies to provide regulatory and compliance support, promoting certainty in relationships, transparency, and trust in market structures.

> "It is activities and risks that attract responsibilities and rules, regardless of the parties involved, in accordance with the principle of proportionality and the aim of not unjustifiably interfering with the potential of technologies."

.

Università Europea di Roma

Co-funded by the European Union

Regulatory Framework of Digital Finance

The European Experience: PSD2 between Successes and Limitations

The European Union has been the main reference point for Open Banking at international level with the introduction of PSD2 in 2015.

Successes of PSD2

- Reduction of fraud thanks to strong authentication
- Secure regulatory framework for TPPs
- Overcoming screen scraping
- Access without a contractual relationship

Limitations highlighted

- Problemi ricorrenti nell'accesso ai dati
- API di bassa qualità e frammentate
- Insoddisfazione di TPP e banche
- Limited use of APIs

EU PSD2, PSD3 and DORA

- The Payment Services Directive 2 (PSD2), adopted in 2015, mandated open access to payment account data and introduced Strong Customer Authentication. Despite its success in enabling third-party providers (TPPs), PSD2 faced challenges: inconsistent implementation across Member States, fragmentation of API standards, and gaps in fraud prevention;
- To address these shortcomings, the European Commission proposed PSD3 and a new Payment Services Regulation (PSR) in 2023. PSD3 strengthens fraud prevention measures, harmonises supervisory practices, and extends the scope toward *Open Finance*, setting the stage for a wider data-sharing ecosystem;
- The Digital Operational Resilience Act (Regulation (EU) 2022/2554) responds to the increasing dependency of financial institutions on digital infrastructure. It imposes obligations on banks, fintechs, and third-party ICT service providers (including cloud providers). Key requirements include incident reporting, digital resilience testing, and contractual oversight of outsourced ICT services. Importantly, DORA subjects “critical” ICT providers to direct supervision by the European Supervisory Authorities (ESAs). Legally, DORA complements PSD2 and PSD3 by ensuring that the open finance ecosystem remains operationally resilient against cyberattacks and systemic ICT failures.

Markets in Crypto-Assets Regulation (MiCA) and the EU AI Act (Genius Act)

- MiCA, adopted in 2023, is the EU's pioneering framework for crypto-assets. It regulates three categories: (1) asset-referenced tokens, (2) e-money tokens, and (3) other crypto-assets such as utility tokens. It excludes security tokens, which fall under MiFID II. MiCA establishes licensing requirements, white paper obligations, governance rules, and reserve mandates for stablecoin issuers. "Significant" issuers face direct supervision by the European Banking Authority (EBA). The regulation aims to create a harmonised single market for crypto-assets, offering legal certainty and consumer protection while reducing regulatory fragmentation across Member States;
- The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) introduces a risk-based framework for AI systems. It prohibits certain practices (such as social scoring by public authorities) and designates others as high-risk. In the financial sector, high-risk applications include credit scoring, fraud detection, and robo-advisory systems. Providers of such systems must implement risk management frameworks, ensure data quality, and maintain human oversight. The Act also requires documentation, transparency, and conformity assessments. For financial services, the AI Act provides a legal structure that both enables innovation and constrains harmful uses of AI.

The UK and the USA Scenarios: A Comparative Lens (1)

- The UK has pursued its own trajectory following Brexit. The Open Banking Implementation Entity (OBIE), created by the UK's Competition and Markets Authority, has overseen implementation since 2016. While similar to PSD2, the UK regime diverges in its technical standards and enforcement mechanisms. The UK government now explores an "Open Finance" agenda to expand access beyond payments. This divergence creates potential compliance challenges for cross-border fintechs, as firms must navigate parallel but distinct regimes;
- The US lacks a comprehensive open banking law. Instead, financial data sharing relies heavily on market-driven practices and bilateral agreements. The Consumer Financial Protection Bureau (CFPB) has signalled interest in developing consumer data rights, but progress remains slow. Big Tech companies play an outsized role in payments innovation, creating both opportunities and antitrust concerns. From a legal perspective, the absence of a harmonised regime contrasts sharply with the EU's regulatory model.

The UK and the USA Scenarios: A Comparative Lens (2)

- Comparing the EU, UK, and US reveals divergent regulatory philosophies. The EU adopts a harmonised, directive- and regulation-driven model. The UK emphasises competition remedies with regulator-led enforcement. The US relies on market-based innovation with limited federal intervention. These differences create challenges for global fintechs, which face fragmented compliance requirements and risks of regulatory arbitrage. International coordination, particularly on stablecoin regulation, is increasingly necessary;
- The EU's digital finance agenda is anchored in multiple instruments: PSD2/PSD3 for open access, DORA for operational resilience, MiCA for crypto-assets, the AI Act for artificial intelligence, and GDPR for data protection. Collectively, these instruments create a layered legal ecosystem. Each instrument addresses a specific domain but interacts with others, requiring careful coordination and harmonisation to avoid overlap, gaps, or conflicting obligations.

.

Università Europea di Roma

Co-funded by the European Union

Crypto-Assets & Stablecoins: An Overview of the Current Legislative Framework

Crypto-Assets and Payment Tokens

- Crypto-assets are defined in MiCA as a digital representation of value or rights that can be transferred and stored electronically using distributed ledger technology (DLT). They serve diverse purposes: payment tokens (digital currencies), utility tokens (access rights), and investment instruments (security tokens).
- MiCA's legal recognition of these categories provides clarity in a previously fragmented regulatory environment, reducing uncertainty for issuers and consumer;
- Payment tokens such as Bitcoin and Litecoin are decentralised and not backed by any underlying assets. They are primarily used for speculation, though some are accepted in retail transactions. EU law does not treat them as legal tender, and under MiCA, they fall outside the stablecoin categories unless they are pegged to assets. Their volatility raises legal questions about consumer protection and systemic risk if they were widely adopted for payments.

Utility Tokens and Security Tokens

- Utility tokens provide access to a digital service or platform, such as Ethereum gas tokens. While useful for funding start-ups through initial coin offerings (ICOs), they often blur the line with investment instruments. MiCA classifies them as crypto-assets requiring disclosure and licensing, but they are not treated as financial instruments unless they exhibit characteristics of securities, in which case MiFID II applies;
- Security tokens represent ownership rights or debt instruments recorded on a blockchain. Unlike utility tokens, they fall squarely within the scope of securities regulation (MiFID II, Prospectus Regulation). They are subject to disclosure obligations, investor protection measures, and licensing rules for intermediaries. The tokenisation of securities raises questions about settlement finality, custody rules, and investor rights in insolvency.

Stablecoins: Definition, Types and Embedded Risks

Co-funded by the European Union

- Stablecoins are designed to maintain a stable value relative to a reference asset. MiCA distinguishes between asset-referenced tokens (pegged to multiple assets, including commodities or crypto) and e-money tokens (pegged to a single fiat currency). Algorithmic stablecoins, which maintain value through code-based supply adjustments, fall outside MiCA's main categories and face restrictions. Examples include USDT (fiat-backed), DAI (crypto-backed), and TerraUSD (algorithmic);
- Stablecoins pose multiple risks: inadequate reserves, mismanagement of backing assets, operational vulnerabilities, and "run" risks if consumer confidence collapses;
  - For instance, the recent TerraUSD collapse illustrates the dangers of algorithmic models. If adopted at scale, stablecoins could undermine monetary policy, create systemic contagion, and challenge financial stability. Regulators respond by imposing prudential and disclosure obligations to mitigate these risks.

The Existing Legal Framework: MiCA's Treatment of Stablecoins

- MiCA imposes strict obligations on issuers of asset-referenced tokens and e-money tokens. Issuers must hold fully backed reserves, guarantee redemption rights, and comply with governance requirements. "Significant" issuers face enhanced supervision by the EBA. Algorithmic stablecoins are largely excluded from use as a payment instrument. These rules ensure that stablecoins integrate safely into the financial system while supporting innovation under controlled conditions;
- The integration of crypto-assets into mainstream finance expands the scope of Open Finance. Indeed, digital wallets can be linked to bank accounts, securities can be tokenised, and decentralised finance (DeFi) platforms can interact with regulated financial institutions. This raises legal challenges regarding custody, liability, and prudential regulation. The EU's strategy seeks to harness crypto innovation while preventing systemic instability and ensuring compliance with anti-money laundering (AML) laws.

Università Europea di Roma

Co-funded by the European Union

Artificial Intelligence and the EU AI Act: Overview, Foundation and Objectives, Challenges and Risks

The Role of AI in Financial Services and the Credit Scoring

- AI applications in finance include automated compliance monitoring, fraud detection, credit risk assessment, and robo-advisory.
- These tools enhance efficiency but raise legal concerns about fairness, bias, and accountability. The AI Act establishes a legal framework for ensuring that these systems are trustworthy and respect fundamental rights;
- AI models allow faster and more accurate credit risk assessments by using large datasets. However, biases in training data can lead to discriminatory outcomes, conflicting with Article 21 of the Charter of Fundamental Rights (non-discrimination). The AI Act designates credit scoring systems as high-risk, subjecting them to strict requirements for transparency, documentation, and human oversight.
  - In this context, robo-advisors start to appear by providing automated investment recommendations to retail clients. While they democratise access to financial advice, they raise questions of liability when advice is unsuitable or leads to losses. Under the AI Act, robo-advisory systems used in finance may be considered high-risk, requiring explainability and monitoring. In parallel, MiFID II continues to apply, ensuring suitability assessments and investor protection.

The EU AI Act ("Genius Act"): Foundations and Objectives

- The EU Artificial Intelligence Act (Regulation (EU) 2024/1689)—informally known as the EU "Genius Act"—is the world's first horizontal regulatory framework for artificial intelligence. It establishes a comprehensive legal regime governing the development, deployment, and use of AI systems across all sectors, including financial services. The Act adopts a risk-based approach, categorising AI systems into four levels: prohibited, high-risk, limited-risk, and minimal-risk;
- In the financial sector, systems used for **credit scoring, fraud detection, algorithmic trading, robo-advisory, and AML monitoring** typically fall under the *high-risk* category, subjecting them to stringent compliance obligations;
- The legal objectives of the Genius Act are twofold:
  - (i) To protect fundamental rights, ensuring that AI systems respect human dignity, privacy, and non-discrimination as guaranteed under the Charter of Fundamental Rights of the European Union; and
  - (ii) To foster trustworthy innovation, ensuring that AI can be safely integrated into critical sectors such as finance, healthcare, and transport without undermining social or economic stability.

Key Provisions of the EU Artificial Intelligence Act: Scope and Definitions

- It applies to AI system providers, users, importers, and distributors operating within the EU, regardless of where the system is developed (extraterritorial reach, similar to GDPR);
- It defines “AI system” broadly to include machine learning, logic-based, statistical, and knowledge-based approaches (Annex I);
- It establishes a risk hierarchy, in detail:
  - Prohibited AI — systems violating fundamental rights or human dignity (e.g., social scoring, manipulative systems, real-time biometric surveillance except under narrow exceptions);
  - High-Risk AI — systems with significant impact on individuals’ rights or safety (e.g., credit scoring, employment, border control, medical devices, financial services);
  - Limited-Risk AI — systems requiring transparency (e.g., chatbots, emotion recognition tools);
  - Minimal-Risk AI — general-purpose or open-source AI not requiring specific obligations.

Key Provisions of the EU Artificial Intelligence Act (2)

- High-risk systems — including those used in creditworthiness assessment, insurance underwriting, algorithmic trading, and fraud prevention — are subject to strict compliance requirements:
  - Risk Management System (Art. 9): Continuous identification, evaluation, and mitigation of AI-related risks.
  - Data Quality and Governance (Art. 10): Training and testing datasets must be complete, accurate, and free from bias; documentation of data provenance required.
  - Technical Documentation (Art. 11–12): Providers must maintain detailed records for traceability and audit.
  - Transparency and Human Oversight (Art. 13–14): Systems must allow human monitoring and intervention; automated decisions must be explainable.
  - Conformity Assessment (Art. 19–23): AI systems must undergo pre-market evaluation and CE marking before deployment.
- These provisions collectively codify the principle of algorithmic accountability — ensuring that AI in finance and other sectors operates within the boundaries of legal predictability and human rights.

Key Provisions of the EU Artificial Intelligence Act (3)

- Recent negotiations introduced obligations for General-Purpose AI (GPAI) and foundation models, such as large language models (LLMs):
  - Providers must document model architecture, training data sources, and energy consumption;
  - High-impact GPAI (e.g., GPT-based systems) must undergo risk assessments and comply with transparency requirements;
  - These rules establish global governance standards for AI infrastructure, extending EU regulatory influence beyond its borders — a clear example of the “Brussels Effect.”;
- In terms of Governance and Sanctions, European Artificial Intelligence Board (EAIB) coordinates national enforcement, issues technical guidance, and harmonises interpretation;
- National Market Surveillance Authorities enforce compliance, conduct audits, and impose administrative sanctions;
- The foreseen penalties are as follows:
  - Up to €35 million or 7% of global turnover for use of prohibited AI systems;
  - Up to €15 million or 3% of global turnover for other breaches.

High-Risk AI Systems in The Genius Act : Compliance Obligations (1)

- The Act's foundation rests on **Articles 114 and 16 TFEU**, enabling the EU to harmonise internal market rules and ensure data protection. In doing so, it situates AI regulation within the EU's constitutional order—balanceng market integration with rights-based governance;
- Within the Genius Act's framework, *high-risk AI systems* are defined by **Articles 6–9**, encompassing any application that can materially affect individuals' access to essential services—such as credit, insurance, or investment advice;
- Financial institutions employing such systems must meet several key obligations:

1. Risk Management System — Firms must establish and maintain a continuous risk management process identifying, analysing, and mitigating risks associated with AI;
2. Data Governance & Quality — Training data must be relevant, representative, free from bias, and regularly updated, ensuring compliance with Article 10 of the Act;
3. Technical Documentation & Record-Keeping — Providers must produce detailed documentation on design, testing, and performance metrics for supervisory review;
4. Transparency & Human Oversight — Users must be informed when interacting with AI, and human oversight must be integrated to override or interpret AI decisions;
5. Conformity Assessment & CE Marking — Before deployment, high-risk AI systems must undergo a conformity assessment to verify compliance with all applicable standards.

High-Risk AI Systems in The Genius Act : Compliance Obligations (2)

- In practice, this means that financial institutions deploying AI-based credit scoring or automated investment tools must maintain both **algorithmic accountability** and **auditability**. Supervisory authorities such as **ESMA**, **EBA**, and **national data protection agencies** will collaborate to ensure coordinated enforcement, creating a new model of **co-regulation** between financial and technology regulators;
- The Genius Act thus operationalises the EU's principle of *technological due process*: the idea that algorithmic systems must be explainable, contestable, and subject to human oversight within the rule of law.

The Genius Act within the EU Digital Finance Constitution (1)

- The European Union is constructing an integrated legal framework that regulates digital finance not through isolated statutes, but through a **constitutional architecture of interlocking regimes;**
- At its core, this framework operationalises three constitutional principles of the EU's digital order:
  - **(1) Technological neutrality**, ensuring the law adapts to innovation without predetermining specific technologies;
  - **(2) Proportionality and risk-based regulation**, tailoring obligations to systemic significance; and
  - **(3) Fundamental-rights integration**, embedding data protection, fairness, and due process into all digital activities.

The Genius Act within the EU Digital Finance Constitution (2)

- Together, these instruments constitute a **multi-layered regulatory stack**:
  - *PSD3* governs **data flows and market access**;
  - *MiCA* governs **digital value and assets**;
  - *DORA* governs **technological infrastructure**;
  - *The Genius Act* governs **algorithmic decision-making**.
- They collectively define the **rights, duties, and constraints** of all actors in the EU digital financial ecosystem;
- The "Digital Finance Constitution" is more than functional coordination; it represents a **constitutionalisation of innovation**. Each pillar reflects a balance between **freedom to innovate** and **responsibility to protect**.

The Genius Act within the EU Digital Finance Constitution (3)

Legal Instrument	Core Domain	Legal Objective	Supervisory Nexus
PSD3 / PSR	Payments & Open Finance	Secure access, consumer consent, competition	EBA + national competent authorities
DORA	Operational & Cyber Resilience	Technological stability, ICT risk management	ESAs + Critical ICT oversight
MiCA	Crypto-Assets & Stablecoins	Market integrity, prudential safeguards, investor protection	ESMA + EBA
Genius Act (AI Act)	Artificial Intelligence Systems	Algorithmic accountability, human oversight, transparency	Cross-sectoral enforcement by ESAs + Data Protection Authorities

The Genius Act: The Constitutional Vision

- This layered structure transforms financial regulation into a **normative ecosystem**: innovation is permitted only within legally secured boundaries that preserve trust and legitimacy;
  - At a meta-level, the EU Digital Finance Constitution represents the Union's distinct regulatory philosophy:
  - **Against laissez-faire deregulation**, it affirms that law must guide markets;
  - **Against technocratic control**, it preserves human agency and accountability;
  - **In favour of responsible innovation**, it frames technology as a public good governed by rights and oversight.
- In effect, the EU no longer merely regulates financial technology — it **governs through technology**, embedding the values of transparency, fairness, and proportionality directly into digital infrastructures and AI systems;
- The Genius Act thus completes the constitutional circle of EU digital finance law: *data access (PSD3), resilience (DORA), value (MiCA), and intelligence (AI Act)* are now unified under one coherent legal vision of **trustworthy, rights-based digital capitalism**.

High-Risk AI Systems and Fraud Detection

- Machine-learning algorithms can detect anomalous transactions and prevent fraud. These systems are essential for compliance with AML Directive 5 (Directive (EU) 2018/843). Yet, they must remain explainable: regulators and courts may require providers to justify how suspicious transactions were flagged. The AI Act ensures transparency obligations, making fraud detection systems auditable;
- In this context, the AI Act (Articles 6–7) classifies credit scoring, fraud detection, and biometric identification in finance as high-risk. Providers must conduct conformity assessments, maintain risk management systems, and log system activity for accountability. These obligations impose compliance costs on fintechs but are designed to safeguard fundamental rights and prevent systemic risks.

Compliance Obligations under AI Act: Innovation vs Burden

- High-risk AI systems must meet several obligations: human oversight, high-quality data to prevent bias, transparency in system design, and technical documentation for audits. The AI Act establishes an EU-wide supervisory system, creating consistency across Member States. For financial institutions, compliance requires alignment with both financial law and AI regulation;
- The AI Act raises concerns about regulatory burden. Strict rules could drive innovation outside the EU to jurisdictions with lighter regimes. Conversely, insufficient regulation could expose consumers to discriminatory or unsafe AI systems. The EU aims to position itself as a global leader in “trustworthy AI,” balancing innovation with rights protection.

Challenges and Risks: Data Privacy & GDPR

- On the one hand, Open Banking interacts with GDPR in complex ways. While PSD2 mandates data sharing, GDPR requires lawful bases, informed consent, and data minimisation. Conflicts arise when banks must share more data than is necessary for a transaction. Regulators stress that PSD2 must be implemented consistently with GDPR, ensuring that consumer consent is specific, informed, and revocable.
- Further, APIs expand the attack surface of financial systems, creating new vulnerabilities. Third-party providers may lack robust security measures, exposing consumers to breaches. DORA addresses these risks by requiring ICT risk management, resilience testing, and third-party oversight. The EU's legal response reflects a recognition that cybersecurity is central to financial stability.

Operational Resilience Challenges: Consumer Consent & Dark Patterns

- The reliance on cloud providers creates concentration risks, as a small number of companies control critical financial infrastructure. DORA subjects “critical ICT third-party providers” to direct EU supervision. Legal obligations include incident reporting, contractual transparency, and resilience stress tests. These measures seek to prevent systemic failures caused by ICT disruptions;
- In this context, a key legal challenge is ensuring that consumer consent is meaningful. Dark patterns—manipulative user interface designs—can pressure consumers into granting consent without full understanding. GDPR requires that consent be freely given, specific, and informed. Supervisory authorities have begun enforcing against misleading consent practices in the fintech sector;
- It is hence understood that financial services are inherently cross-border, but regulation remains fragmented. Stablecoin issuers, for example, may exploit jurisdictional differences to avoid strict obligations. This regulatory arbitrage undermines consumer protection and financial stability. International coordination, particularly through the Financial Stability Board (FSB), is essential for consistent global standards.

Operational Resilience Challenges: Financial Stability Concerns

- The progressive opening of financial data and services under the Open Finance model introduces complex systemic risks that challenge the traditional prudential architecture of EU financial regulation. By enabling the interconnection of banks, fintechs, and third-party providers through APIs, Open Finance increases efficiency and innovation but also creates new channels for contagion;
- A cyber incident or operational failure in one node—such as a cloud provider or payment service interface—can propagate rapidly across the ecosystem, amplifying systemic vulnerabilities. Similar risks arise in crypto-markets: the collapse of algorithmic stablecoins like TerraUSD (2022) demonstrated how unregulated digital assets can trigger liquidity shocks and erode market confidence;
- In this context, MiCA addresses part of this challenge by imposing prudential and liquidity requirements on issuers of asset-referenced and e-money tokens, thereby aligning them with the principles of Basel III and the EBA's prudential standards. Yet, further gaps remain concerning decentralised finance (DeFi) and cross-border oversight;
- In parallel, the Digital Operational Resilience Act (DORA) strengthens systemic protection by mandating ICT risk management and resilience testing for all financial entities and critical third-party providers. From a policy standpoint, these developments illustrate the EU's evolving regulatory philosophy: systemic stability in digital finance can no longer rely solely on capital adequacy or traditional supervision—it must integrate technological resilience, cross-sector oversight, and macroprudential monitoring of digital ecosystems.

Risks and Opportunities of Digital Innovation

Opportunities

- More financial inclusion;
- Customized services based on data;
- Switching costs reduction;
- Better control of personal finances;
- More convenient and competitive offers

Major Risks for Less Protected Consumers

- Discrimination coming from the use of algorithms;
- Manipulation and illegit exploitation;
- Poor level of digital knowledge;
- Opacity around Automated Decisions

Warning: The digitization of financial transactions increases the risk of discrimination and exploitation of the most vulnerable customers, requiring particular attention in the design of safeguards.

Competitive Impacts and Systemic Concerns

FinTech

They benefit from access to data but often collaborate with traditional banks rather than compete with them.

Aggregators

They emerge as intermediaries but create risks of market concentration

BigTech Companies

They pose a real competitive threat, leveraging proprietary data silos and advanced analytical capabilities.

Traditional Banks

They are subject to asymmetric data sharing obligations without reciprocity on the part of TPPs.

Data sharing obligations have encouraged the entry of BigTech companies, which initially entered the market through payment services but quickly diversified into credit, insurance, and investments.

Technical Challenges: API Standardisation

One of the most debated issues concerns API standardization: should a common standard be imposed or should the market be left free?

In favour of Standardization

Reduction of interoperability costs and barriers for new market entrants

Against Standardization

Risk of compromising dynamic competition between standards and undermining incentives for innovation

The fragmentation of API standards can exacerbate the costs of interoperability, compounded by the lack of incentives for banks to grant access to TPPs.

2

Main Standards

In Europe, there is an actual convergence to Berlin Group and STET Standard standard STET

9

CMA9 Banks

Common API Standards have been agreed in the United Kingdom

Università Europea di Roma

Co-funded by the European Union

Regulatory Proposals and Policy Considerations within the European Union

Regulatory Harmonisation and API Interoperability

- The coexistence of PSD3, MiCA, GDPR, DORA, and the AI Act creates risks of overlap and fragmentation. Harmonisation is essential to reduce compliance complexity for firms and ensure consistency for consumers. Proposals include coordinated supervisory mechanisms and integrated guidance documents from the European Supervisory Authorities.
- Standardised APIs are essential for cross-border Open Finance. Without uniform standards, fragmentation undermines competition. The EU could legislate technical API standards or support industry-driven harmonisation, building on initiatives such as the Berlin Group's "NextGenPSD2" standard.
  - Regulatory sandboxes allow innovative firms to test new products under supervisory oversight. This model, pioneered by the UK's Financial Conduct Authority, is increasingly adopted in the EU. Sandboxes balance innovation with consumer protection by enabling real-world experimentation in a controlled environment.

Prudential Treatment of Stablecoins

- The prudential treatment of stablecoins has emerged as one of the most pressing issues in digital finance law. Stablecoins—crypto-assets designed to maintain a stable value relative to a reference asset—occupy an ambiguous space between payment instruments, securities, and deposits;
- MiCA provides a landmark attempt to fill this regulatory gap by distinguishing between asset-referenced tokens (ARTs) and e-money tokens (EMTs). ARTs are backed by multiple assets (e.g., baskets of fiat and commodities), while EMTs are pegged to a single fiat currency and legally resemble electronic money under Directive 2009/110/EC (E-Money Directive II);
- Under MiCA, issuers of both categories must maintain fully backed reserves, implement transparent governance structures, and guarantee redemption rights at par value. Critically, “significant” stablecoin issuers—those whose tokens reach systemic importance—are subject to direct supervision by the European Banking Authority (EBA) and additional capital and liquidity requirements. These prudential measures mirror the core principles of Basel III—capital adequacy, liquidity coverage, and operational resilience—but are tailored to the digital nature of the assets;
- In essence, the prudential treatment of stablecoins seeks to reconcile innovation with stability by applying traditional financial safeguards to novel instruments. The goal is to embed digital asset markets within the EU’s existing prudential order, ensuring that financial innovation evolves within a safe, legally sound environment.

Open Finance and the Cross-Sector Alignment (1)

- Open Finance cannot function in isolation; its long-term success depends on cross-sector legal alignment with the EU's broader data governance architecture. Financial data sharing under PSD2 and the upcoming PSD3 intersects with the horizontal frameworks established by the Data Governance Act (Regulation (EU) 2022/868), the Data Act (Regulation (EU) 2023/2854), and the European Data Strategy (COM/2020/66 final). These instruments collectively aim to create a Single Market for Data, promoting interoperability, transparency, and consumer control across all economic sectors—not only finance;
- The Data Governance Act establishes mechanisms for data intermediaries, data altruism organisations, and public-sector data re-use, ensuring that data sharing occurs within trustworthy environments. Meanwhile, the Data Act provides horizontal rules on business-to-business and business-to-consumer data access, imposing interoperability standards and mandating fair contractual terms for data sharing. These general-purpose regulations complement PSD3's sector-specific rules, ensuring that financial data portability aligns with broader EU digital policy;
- However, legal challenges arise from overlapping obligations and differing definitions of consent, control, and portability. For example, GDPR's personal data regime operates in parallel with the Data Act's focus on non-personal data, creating interpretative uncertainty for mixed datasets. To address this, the European Commission's Digital Finance Strategy (COM/2020/591 final) advocates an "open but safe" approach, where cross-sector interoperability is pursued without compromising privacy, competition, or cybersecurity.

Open Finance and the Cross-Sector Alignment (2)

- However, legal challenges arise from overlapping obligations and differing definitions of consent, control, and portability. For example, GDPR's personal data regime operates in parallel with the Data Act's focus on non-personal data, creating interpretative uncertainty for mixed datasets. To address this, the European Commission's Digital Finance Strategy (COM/2020/591 final) advocates an "open but safe" approach, where cross-sector interoperability is pursued without compromising privacy, competition, or cybersecurity;
- From a regulatory perspective, cross-sector alignment ensures that innovations in Open Finance can scale beyond payments and banking into adjacent domains such as insurance, energy, and health. This convergence supports the EU's strategic goal of achieving data sovereignty—a legal framework where European values, rights, and standards govern the digital economy. The task ahead for legislators is to ensure that sector-specific financial laws like PSD3 and MiCA remain harmonised with the horizontal data governance framework, avoiding legal fragmentation while promoting innovation.

The Prospect Outlook and Future Directions

Open Finance to Open Data Economy (1)

- The evolution from *Open Banking* to *Open Finance* marks only the first stage in the EU's ambition to build a comprehensive Open Data Economy, where data flows seamlessly across sectors under harmonised governance frameworks. The European Commission's European Data Strategy (COM/2020/66 final) envisions a single market for data as the cornerstone of Europe's digital transformation. Within this framework, the Data Governance Act (Regulation (EU) 2022/868) and the Data Act (Regulation (EU) 2023/2854) play a pivotal role in creating cross-sector interoperability. They establish rules for data sharing across public and private entities, enabling data re-use beyond finance — including in energy, health, mobility, and agriculture;
- In legal terms, Open Finance can be seen as a *sector-specific pilot* for this broader model. The Payment Services Directive 2 (PSD2) operationalised the right to data portability (Article 20 GDPR) in the banking sector, compelling institutions to share customer data via APIs. The forthcoming Payment Services Directive 3 (PSD3) and Financial Data Access Regulation (FIDA) aim to extend this model to all financial products, laying the foundation for a multi-sector "data space" governed by shared interoperability standards.

Open Finance to Open Data Economy (2)

- The legal challenge, however, lies in balancing openness with sovereignty and security. The EU's "open but protected" model seeks to ensure that European data infrastructures remain independent of extra-EU technological dominance—particularly from U.S. and Chinese BigTech platforms—by embedding principles of *data sovereignty*, *trust*, and *fundamental rights*. This approach distinguishes the EU from the market-driven U.S. model and the state-controlled Chinese model, positioning it as a third regulatory paradigm based on constitutional safeguards;
- From a policy perspective, the transition toward an Open Data Economy requires reconciling sectoral regulations like PSD3, MiCA, and DORA with horizontal frameworks such as the Data Act and GDPR. This ensures that financial data sharing aligns with broader data governance principles of fairness, competition, and protection of personal rights. Ultimately, Open Finance serves as both a test case and a catalyst for the EU's vision of a trusted, rights-based digital economy — one that harnesses data as a common good rather than a proprietary asset.

Central Bank Digital Currencies (1)

- The rise of digital assets and the growing adoption of private stablecoins have prompted central banks worldwide to explore Central Bank Digital Currencies (CBDCs) — sovereign digital money issued directly by a central bank and representing a direct claim on the state. Unlike cryptocurrencies or stablecoins, CBDCs are legal tender, backed by the monetary authority, and serve as a risk-free public payment instrument. Within the European Union, the European Central Bank (ECB) has advanced its research and design phase for a potential Digital Euro, aimed at complementing—not replacing—cash;
- The legal foundation for a Digital Euro rests on Articles 127 and 128 of the TFEU, which establish the ECB's mandate to maintain price stability and authorise it to issue euro banknotes and coins. Extending this authority to a digital form of central bank money requires new secondary legislation, as physical issuance does not automatically cover electronic equivalents. In June 2023, the European Commission proposed a Regulation on the Establishment of the Digital Euro (COM/2023/369 final), setting out the legal framework for issuance, distribution, and privacy safeguards. The proposal confirms that the digital euro would be legal tender across the euro area and accessible to citizens and businesses through intermediaries such as banks and payment institutions.

Central Bank Digital Currencies (2)

- The policy rationale for a Digital Euro is multifaceted. First, it preserves the role of public money in an increasingly digital economy dominated by private payment systems and foreign providers (e.g., Visa, Mastercard, PayPal). Second, it enhances monetary sovereignty by providing a European alternative to private stablecoins or non-EU digital currencies. Third, it promotes financial inclusion, ensuring that all citizens—regardless of access to commercial banking—can use risk-free digital payments. Finally, it serves as a strategic response to the proliferation of digital assets, preventing monetary fragmentation and ensuring the uniformity of the euro;
- However, CBDCs also raise profound legal and economic challenges. One central concern is financial disintermediation: if citizens can hold deposits directly with the central bank, commercial banks may lose a significant portion of their funding base, destabilising the traditional credit intermediation model. The ECB has therefore proposed limits on individual holdings and designed an intermediated architecture, whereby private financial institutions distribute and manage CBDC accounts while the ECB maintains the ledger and monetary control. Another issue is privacy. Unlike cash, CBDCs can be traced electronically, raising concerns about surveillance and data protection. The proposed regulation introduces privacy-by-design principles and compliance with the General Data Protection Regulation (GDPR), ensuring that the digital euro provides a “cash-like” level of privacy for low-value transactions while maintaining traceability for anti-money laundering (AML) purposes.

Central Bank Digital Currencies (3)

- From a global perspective, CBDCs are also instruments of geopolitical and regulatory competition. China's e-CNY, the United States' research on a "digital dollar," and initiatives by the Bank for International Settlements (BIS) and IMF illustrate a worldwide race to redefine the future of money. The EU's approach, grounded in legal certainty and rights protection, seeks to balance innovation with constitutional safeguards, reinforcing the euro's global credibility;
- To wrap up, the Digital Euro exemplifies the EU's strategy of *regulating through design*. It translates fundamental monetary and constitutional principles into digital architecture—ensuring that the transition to a cashless economy preserves the legal integrity, inclusivity, and sovereignty of the monetary system. As such, the CBDC debate is not merely technical or economic; it is profoundly constitutional, redefining the legal relationship between the citizen, the market, and the state in the digital age.

The Advent of Decentralised Finance and Its Challenges (1)

- Decentralised Finance (*DeFi*) represents one of the most profound legal challenges to existing financial regulation. Built on public blockchain networks, DeFi systems enable peer-to-peer lending, trading, and asset management without intermediaries such as banks or brokers. Instead, they rely on *smart contracts* — self-executing code that automatically enforces agreements. This decentralised structure poses deep questions for EU financial law, which traditionally assigns responsibility to identifiable legal persons subject to licensing and supervision;
- Under current EU law, DeFi largely falls outside the scope of MiCA (Regulation (EU) 2023/1114), which applies to identifiable issuers and intermediaries. Pursuant to Article 2(5) MiCA, "fully decentralised" systems without a central issuer or service provider are excluded. This regulatory gap means that DeFi platforms—such as decentralised exchanges (DEXs) or automated lending protocols—often operate in a grey zone, exposing users to unmitigated market and operational risks. Moreover, DeFi's reliance on pseudonymous participants raises concerns under EU Anti-Money Laundering (AML) Directives, particularly Directive (EU) 2018/843 (AMLD5), which mandates customer identification and transaction monitoring.

The Advent of Decentralised Finance and Its Challenges (2)

- Smart contracts also challenge core legal doctrines. Questions of jurisdiction, enforceability, and liability become difficult when the "contract" is code deployed on a borderless network. If a DeFi lending protocol fails, who is legally accountable—the developers, the DAO (Decentralised Autonomous Organisation), or the token holders? EU private law offers limited guidance, as traditional contract doctrines presume human intent and identifiable parties. Furthermore, DeFi governance mechanisms (through token voting) raise issues of collective responsibility, investor protection, and compliance with securities law when governance tokens function like shares or voting right;
- Regulators have begun exploring potential responses. The **European Securities and Markets Authority (ESMA)** and the **European Banking Authority (EBA)** have recommended extending certain MiCA obligations to DeFi actors that exert "effective control" over a protocol, even if decentralised in form. The **Financial Stability Board (FSB)** has likewise warned that large-scale DeFi systems could replicate systemic risks of traditional finance—leverage, liquidity mismatches, and contagion—without equivalent safeguards.
- From a policy standpoint, the EU faces a delicate task: how to regulate decentralised markets without extinguishing innovation. Proposals include *embedded compliance* (regulation via code), *legal recognition of DAOs* as corporate entities, and *selective supervision* of critical DeFi infrastructures such as decentralised stablecoins or liquidity pools.

The Phenomenon of the Tokenisation of Real Assets (1)

- The tokenisation of real assets represents a fundamental shift in how property rights, ownership, and value are represented and transferred within the European Union's legal and financial systems. Tokenisation refers to the process of issuing a digital representation of an asset on a distributed ledger (DLT), effectively converting real-world assets—such as real estate, commodities, equity, or bonds—into digital tokens that can be transferred, divided, and traded electronically. From a legal perspective, this process challenges the existing categories of private and financial law by introducing a new layer of digital intermediated ownership, where rights in tangible assets are represented by cryptographic tokens rather than traditional legal titles;
- Within the EU legal framework, tokenisation engages multiple intersecting regimes. Where the tokenised asset confers rights analogous to shares, bonds, or other financial instruments, it falls within the scope of MiFID II (Directive 2014/65/EU) and the Prospectus Regulation (EU) 2017/1129), requiring disclosure, investor protection, and licensing obligations. When tokenisation is applied to instruments traded on DLT platforms, the DLT Pilot Regime (Regulation (EU) 2022/858) provides an experimental legal environment for market infrastructures—such as multilateral trading facilities (MTFs) and central securities depositories (CSDs)—to operate using blockchain technology under regulatory supervision. This pilot regime, effective since March 2023, temporarily relaxes certain provisions of the Central Securities Depositories Regulation (CSDR) and MiFIR, enabling tokenised trading and settlement systems to function within controlled conditions.

The Phenomenon of the Tokenisation of Real Assets (2)

- The legal innovation of tokenisation lies in its potential to enhance efficiency, transparency, and accessibility. By allowing fractional ownership, tokenisation lowers entry barriers for small investors, democratising access to traditionally illiquid asset classes like real estate or fine art. Additionally, the immutable and transparent nature of distributed ledgers reduces settlement times, counterparty risk, and operational costs. However, these benefits come with legal complexities. The transfer of ownership in tokenised assets raises questions about the recognition of on-chain transactions under property and contract law—particularly whether a blockchain record constitutes legal proof of title or merely evidence of it. Moreover, the lex loci rei sitae (the law of the place where the property is located) traditionally governs rights in immovable property, posing jurisdictional conflicts when tokens representing such assets circulate globally;
- Custody of tokenised assets presents another unresolved issue. Traditional custodianship relies on possession or control of physical certificates or dematerialised securities held in centralised systems. In a blockchain context, control is exercised through private keys, making possession and loss legally ambiguous. The European Banking Authority (EBA) and European Securities and Markets Authority (ESMA) are exploring how existing custody and safekeeping rules—such as those in the Central Securities Depositories Regulation (CSDR)—might apply to tokenised instruments. Questions of insolvency protection, segregation of client assets, and fiduciary duties must be reinterpreted in light of decentralised architectures.

The Phenomenon of the Tokenisation of Real Assets (3)

- Furthermore, tokenisation blurs the line between financial and non-financial assets. While tokenised bonds or shares fit comfortably within securities law, tokens representing ownership of physical assets (e.g., real estate or art) may fall outside MiFID II but still raise consumer protection and AML concerns. The European Commission's Digital Finance Package (2020) recognises this complexity, calling for a "technology-neutral" regulatory approach—one that focuses on function rather than form. This principle underlies both MiCA and the DLT Pilot Regime: the legal treatment of a token depends on its economic function, not its technological structure;
- Finally, tokenisation has macroeconomic and systemic implications. By increasing market efficiency and liquidity, it may also facilitate greater leverage, cross-asset correlations, and rapid contagion during crises. These risks underscore the need for prudential oversight, data transparency, and operational resilience—objectives addressed by DORA (Regulation (EU) 2022/2554). Tokenisation thus sits at the intersection of innovation and regulation: it promises to modernise capital markets but requires careful legal calibration to ensure that property rights, investor protection, and systemic stability remain intact.

Recent Case Studies from the UK and the EU

The British Model and The Advent of Open Finance

Co-funded by the European Union

UK Standardized Model

The United Kingdom has opted for a more invasive implementation with common API standards agreed upon by the nine largest banks (CMA9).

Positive Results

Over 7 million consumers and businesses use Open Banking services, with high customer satisfaction.

Active Users

Consumers and businesses using Open Banking services in the United Kingdom

SMEs Involved

Small and medium-sized enterprises benefiting from services

EU FIDA Proposal

The European Commission has presented a proposal to extend Open Banking to Open Finance, based on the same logic as PSD2 but learning from its limitations.

United Kingdom: Open Banking (1)

- The United Kingdom was the pioneer of Open Banking, establishing the world's first comprehensive regulatory and technical framework for data-driven financial innovation. The initiative originated from the 2016 Retail Banking Market Investigation conducted by the UK Competition and Markets Authority (CMA), which identified significant barriers to competition and consumer mobility in the retail banking sector. In response, the CMA issued the Retail Banking Market Investigation Order 2017, mandating the nine largest UK banks (the "CMA9") to share customer account and payment data with licensed third-party providers via secure application programming interfaces (APIs);
- To operationalise this framework, the CMA established the Open Banking Implementation Entity (OBIE) — a non-profit organisation governed by the UK's nine major banks under regulatory oversight. The OBIE developed technical API standards, customer consent protocols, and data security frameworks that would become global benchmarks for Open Banking ecosystems. The legal foundation of this regime was aligned with the EU's PSD2 (Directive (EU) 2015/2366), but its design was more prescriptive and centralised. Whereas PSD2 provided broad obligations and left implementation to Member States, the UK mandated uniform API specifications and a single governance entity, ensuring faster and more consistent adoption.

United Kingdom: Open Banking (2)

- Post-Brexit, Open Banking remains a cornerstone of the UK's financial innovation strategy, now evolving into the broader framework of Open Finance and eventually Smart Data. In 2023, the Joint Regulatory Oversight Committee (JROC)—comprising the Financial Conduct Authority (FCA), the Payment Systems Regulator (PSR), the HM Treasury, and the Competition and Markets Authority—published a roadmap to expand Open Banking into pensions, mortgages, and insurance, thereby mirroring the EU's forthcoming Financial Data Access Regulation (FIDA);
- Despite its success in fostering innovation, challenges persist. Consumer adoption remains limited—fewer than 15% of UK consumers actively use Open Banking services—and cybersecurity incidents have exposed vulnerabilities in third-party provider ecosystems;
- From a legal and policy perspective, the UK model demonstrates both the promise and pitfalls of data-driven financial reform. Its centralised governance and standardised API model have been highly effective, but the regime's sustainability now depends on ensuring consumer trust, strengthening cybersecurity, and integrating Open Banking into the broader UK Smart Data economy. The post-Brexit divergence between UK and EU frameworks also raises cross-border compliance challenges for fintech firms operating in both markets, underscoring the need for regulatory interoperability in the evolving global Open Finance landscape.

European Union: Crypto Regulation under MiCA (1)

- The Markets in Crypto-Assets Regulation (MiCA, Regulation (EU) 2023/1114) marks a watershed moment in global financial regulation, positioning the European Union as the first major jurisdiction to adopt a comprehensive legal framework for crypto-assets. Before MiCA, the EU's approach to digital assets was fragmented: certain instruments fell under existing financial regulations such as MiFID II, E-Money Directive II, or the Prospectus Regulation, while others—particularly utility and payment tokens—remained unregulated. This regulatory asymmetry created uncertainty for issuers, investors, and supervisors, impeding market development and consumer protection;
- MiCA addresses this gap by creating a harmonised regime that applies across all 27 Member States. It distinguishes three main categories of crypto-assets:
  - Asset-Referenced Tokens (ARTs) — crypto-assets pegged to baskets of assets (such as commodities, fiat currencies, or other crypto-assets);
  - E-Money Tokens (EMTs) — crypto-assets linked to a single fiat currency and functioning as a means of payment; and
  - Other Crypto-Assets — including utility tokens that grant access to digital platforms or services.

European Union: Crypto Regulation under MiCA (2)

- Issuers of these tokens must comply with detailed obligations regarding authorisation, governance, transparency, and consumer protection. Each public offering of crypto-assets requires a white paper (analogous to a prospectus) containing essential information about the issuer, the token's features, risks, and technology. These white papers must be approved by the competent national authority and notified to the European Securities and Markets Authority (ESMA);
- For stablecoin issuers (ARTs and EMTs), MiCA introduces additional prudential and operational requirements. Issuers must maintain fully backed reserves in low-risk, liquid assets and guarantee redemption rights at par value. Where stablecoins are deemed "significant" in size or systemic relevance, the European Banking Authority (EBA) assumes direct supervisory responsibility, mirroring the prudential oversight applied to traditional financial institutions. MiCA also prohibits interest payments on stablecoins and limits their use as a widespread means of payment to preserve monetary sovereignty and financial stability—especially vis-à-vis the forthcoming Digital Euro.
- MiCA's scope explicitly excludes certain activities, such as fully decentralised finance (DeFi) protocols and non-fungible tokens (NFTs), though the European Commission has committed to re-examining these sectors within 18 months of MiCA's entry into force. Moreover, MiCA operates alongside other components of the Digital Finance Package (2020)—including DORA, which ensures digital resilience, and the Transfer of Funds Regulation (TFR, Regulation (EU) 2023/1113), which extends anti-money laundering (AML) requirements to crypto transactions.

European Union: Crypto Regulation under MiCA (3)

- From a legal and policy standpoint, MiCA serves several objectives. First, it enhances legal certainty by creating uniform definitions and obligations across Member States, preventing regulatory arbitrage. Second, it strengthens consumer protection through disclosure and prudential safeguards. Third, it promotes financial innovation by providing a stable regulatory environment for legitimate crypto businesses. Finally, it consolidates the EU's strategic autonomy by establishing itself as a global standard-setter for digital asset regulation, influencing emerging frameworks in the UK, Switzerland, Singapore, and the U.S;
- In effect, MiCA reflects the EU's characteristic *"constitutionalisation of innovation"*—embedding technological progress within a rights-based and prudential legal order. It reconciles market dynamism with stability and trust, affirming the EU's regulatory philosophy that innovation must operate within clear legal boundaries.

Need for a Global Coordination (?)

- Digital finance and crypto-assets are inherently borderless, but financial regulation remains deeply territorial. This structural tension gives rise to regulatory fragmentation, jurisdictional arbitrage, and uneven consumer protection standards across the globe. As stablecoins, crypto exchanges, and decentralised finance (DeFi) platforms operate transnationally, no single jurisdiction can ensure market integrity or systemic stability in isolation. The need for global coordination in digital finance is therefore both a legal and policy imperative.
- The European MiCA represents a pioneering regional framework, but its effectiveness ultimately depends on the alignment of international standards. The Financial Stability Board (FSB), the International Monetary Fund (IMF), and the Bank for International Settlements (BIS) have each recognised that uncoordinated national approaches to crypto regulation create systemic vulnerabilities. The FSB's High-Level Recommendations on the Regulation, Supervision and Oversight of Global Stablecoin Arrangements (2020) and its 2023 Global Framework for Crypto-Asset Activities call for consistent prudential, conduct, and disclosure standards across jurisdictions. These recommendations have been formally endorsed by the G20 Finance Ministers and Central Bank Governors, signalling a growing consensus around the need for international coherence.

Need for a Global Coordination (?)

- However, practical implementation remains uneven. The United States continues to regulate digital assets primarily through enforcement actions by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) rather than through comprehensive legislation. This case-by-case approach leads to legal uncertainty and inconsistent classification of tokens as securities or commodities. In contrast, the United Kingdom and Switzerland have pursued more principle-based frameworks, focusing on innovation-friendly supervision and proportionate risk management. Singapore, under the Payment Services Act (2019), and Japan, under the Payment Services Act and Financial Instruments and Exchange Act, have introduced licensing regimes that closely resemble MiCA's risk-based model, but with varying levels of consumer protection and AML requirements;
- These divergences create challenges for cross-border enforcement and regulatory equivalence. For instance, a stablecoin issuer authorised under MiCA may not automatically meet licensing conditions in the United States or Asia, leading to duplicative compliance costs and fragmented market access. Moreover, the lack of harmonisation complicates the supervision of global crypto intermediaries, such as exchanges or custodians, that operate across multiple jurisdictions with inconsistent reporting and capital standards.

Need for a Global Coordination (?)

- The EU's approach, grounded in legal certainty and prudential alignment, positions it as a normative leader in global digital finance governance. Through the "Brussels Effect", EU regulations often set de facto global standards, influencing third countries and international organisations. This phenomenon is already visible in the growing adoption of MiCA-like frameworks in Latin America (e.g., Brazil's 2024 Virtual Assets Law). Nevertheless, EU unilateralism carries risks: without reciprocal recognition or cooperation mechanisms, global financial integration could splinter into regulatory blocs, undermining efficiency and innovation.
- To address this, policymakers and international institutions are exploring several coordination mechanisms. These include:
  - Mutual recognition frameworks allowing cross-border passporting of licences between jurisdictions with equivalent regulatory safeguards;
  - Global reporting and disclosure standards for crypto-assets, modelled on the Basel Committee's prudential frameworks;
  - Joint supervisory colleges for major crypto service providers and stablecoin issuers, akin to those used for global systemically important banks (G-SIBs); and
  - Enhanced data-sharing and technical cooperation under the FSB, IOSCO, and BIS Innovation Hub.

Need for a Global Coordination (?)

- Ultimately, global coordination in digital finance is not only about harmonising technical standards but also about reconciling differing **regulatory philosophies**. The EU prioritises consumer protection and systemic stability through law; the U.S. emphasises market efficiency and enforcement discretion; and Asia often focuses on technological competitiveness and inclusion. The challenge for international law is to bridge these paradigms without diluting the core values of each;
- In conclusion, global coordination is indispensable for a resilient and fair digital financial ecosystem. As digital assets and AI-driven financial systems transcend national borders, international law must evolve from reactive harmonisation to proactive governance. The **EU's MiCA and DORA frameworks**, coupled with global dialogue through the **G20** and **FSB**, represent the first steps toward an emerging *lex digitalis financea* — a nascent body of transnational norms for the digital financial order.

Università Europea di Roma

Co-funded by the European Union

Conclusions

The Paradox of Openness

- The principle of *openness* lies at the heart of the EU's digital finance strategy — yet it is also the source of its deepest contradictions. Openness fosters competition, innovation, and inclusion, but it simultaneously introduces fragility, complexity, and new risks to financial stability and data protection. This duality forms what may be called the paradox of openness: the more interconnected and transparent a financial ecosystem becomes, the more exposed it is to systemic shocks, privacy breaches, and regulatory fragmentation;
- At a conceptual level, the PSD2 embodies this paradox. By mandating open access to customer account data for licensed third-party providers, PSD2 democratised financial services and catalysed the fintech revolution. However, it also created new vectors for fraud, operational failure, and data misuse. Each layer of connectivity — new APIs, data intermediaries, and open infrastructures — multiplies potential points of vulnerability. This mirrors a broader tension in financial law between market liberalisation and prudential control: openness expands opportunity, but each expansion demands new regulatory safeguards.

The Paradox of Openness

- This paradox is further evident in the regulation of crypto-assets. MiCA opens EU markets to digital innovation by providing a clear legal framework for token issuance and trading. Yet, by legitimising these activities, it also integrates crypto markets into the regulated financial system, importing volatility and contagion risks that were previously isolated. Similarly, the EU AI Act (Regulation (EU) 2024/1689) opens the door to algorithmic decision-making in finance while simultaneously classifying key AI applications—such as credit scoring and fraud detection—as "high-risk," imposing strict compliance burdens.
- Ultimately, the paradox of openness underscores the maturity of the EU's digital finance law. Regulation in this space is not simply about enabling competition but about constructing a *sustainable architecture of trust*. Openness, in the EU legal tradition, is not an end in itself—it is a regulated condition for legitimate participation in a digital economy built on fundamental rights, consumer protection, and systemic stability.

Regulation as Enabler, Not Constraint

- Contrary to some of the critics seeing regulation to stifle innovation, the evolution of EU digital finance law illustrates that regulation can serve as an enabler—a legal infrastructure that provides certainty, trust, and legitimacy for technological and market development. The success of Open Banking and Open Finance in the European Union rests precisely on this principle: legal frameworks did not emerge to restrict innovation but to make it possible within a coherent and trustworthy system;
- The PSD2 and its successor PSD3 exemplify this enabling function. By creating a harmonised licensing regime for payment initiation and account information services, the EU transformed fintech from a legal grey zone into a regulated market. Clear rules on data access, consent, and liability gave fintech firms the legal confidence to innovate and attract investment. Similarly, the MiCA replaces regulatory uncertainty with a predictable compliance regime, thereby lowering barriers to entry for legitimate actors and discouraging illicit or speculative practices. Regulation here functions not as a constraint on innovation but as a coordination mechanism that aligns private initiative with public trust.

Regulation as Enabler, Not Constraint

- From a legal perspective, this approach reflects the **European legal tradition of "ordo-liberalism"**—the belief that markets function best when embedded in a strong legal order that ensures fairness, stability, and predictability. The EU's approach to digital finance law—through instruments such as the **DORA**, the **GDPR** and the **AI Act**—translates this philosophy into the digital age. Each of these frameworks imposes obligations, but also creates the conditions for confidence: consumers trust that their data is protected; investors trust that systemic risks are managed; innovators trust that compliant business models will not be undermined by legal uncertainty;
- In practice, the enabling role of regulation manifests in three ways:
  - Certainty — Clear, harmonised rules reduce transaction costs and compliance ambiguity, fostering cross-border scalability;
  - Trust — Strong safeguards build consumer and investor confidence, which is indispensable for digital adoption; and
  - Legitimacy — Regulatory compliance signals market maturity and integrity, attracting both users and institutional capital.

Conclusions

- Far from being an impediment, regulation thus functions as the *constitutional infrastructure* of digital finance. It defines the “rules of the game” in a way that supports innovation, rather than suppressing it. As the EU transitions from Open Banking to Open Finance and ultimately toward a broader Open Data Economy, the legal framework will remain the enabling architecture upon which trust, competition, and technological progress depend. In this sense, regulation is not the opposite of innovation—it is its precondition.

Università Europea di Roma

Co-funded by the European Union

Conclusions

Analysis of the European experience with Open Banking confirms that designing an appropriate regulatory framework involves delicate policy choices that require a tailored approach.

1 Balanced Approach

Policy makers should adopt tailor-made solutions, taking into account the specific characteristics of the relevant geographical market and the results of other experiences.

2 Interests Balance

It is necessary to carefully weigh the advantages and disadvantages of market-led versus regulatory-led regimes, balancing innovation, competition, and consumer protection.

3 Lessons Learned

The PSD2 experience demonstrates the importance of standardization, API quality, and incentive management for all market players.

> "One size does not fit all" - The motivations, objectives, and challenges of Open Banking suggest that there is no universal solution that works for all contexts.

The future of Open Banking and Open Finance will depend on regulators' ability to strike the right balance between promoting innovation, safeguarding competition, and protecting consumers, tailoring solutions to the specific characteristics of each market.

Essential Bibliography

- Armour, John et al., "*FinTech and the Future of Financial Regulation*", Oxford Journal of Legal Studies (2021).
- **Arner, Douglas W., Barberis, Janos, and Buckley, Ross P.**, *"The Evolution of FinTech: A New Post-Crisis Paradigm?"*, **Georgetown Journal of International Law**, Vol. 47, 2016, pp. 1271–1320;
- **Brummer, Chris & Yadav, Yesha**, *"FinTech and the Innovation Trilemma"*, **Georgetown Law Journal**, Vol. 107, 2019, pp. 235–307.
- Busch, Danny, European Financial Regulation and Supervision: *Institutional Design and Policy Challenges* (Oxford University Press, 2022).
- Corea, F., Fossa, F., Loreggia, A. et al. — *"A principle-based approach to AI: the case for European Union and Italy"*, **AI & Society** 2023
- Dirk Zetzsche & Ross Buckley, "*Regulating FinTech: Principles, Challenges, and Policy Responses*", University of Luxembourg Law Working Paper (2020).
- **Ferran, Eilís**, *"Regulating Crypto-Assets in the EU: The Significance of MiCA"*, **European Business Organization Law Review**, Vol. 25(2), 2024.
- Genovese, Anna., Falce, Valeria et al., "*La portabilità dei dati in ambito finanziario (Data Portability in the Financial Sector)*", CONSOB Fintech Series No. 8, 2021.
- Veale, Michael & Edwards, Lilian, "*Clarity, Compliance, and Consequences: The EU AI Act and the Future of Algorithmic Regulation*", Common Market Law Review (2023).
- Brummer, Chris & Yadav, Yesha, "*FinTech and the Innovation Trilemma*", Georgetown Law Journal (2019).
- Ferran, Eilís, "*Regulating Crypto-Assets in the EU: The Significance of MiCA*", European Business Organization Law Review (2024).
- Moloney, Niamh, *EU Financial Market Regulation in the Age of Digitalisation* (Cambridge University Press, forthcoming 2025).
- Sciarrone Alibrandi, A., Rabitti, M., & Schneider, G. — *"The European AI Act's Impact on Financial Markets: From Governance to Co-Regulation"* (2023) by Gabriele Mazzini & Francesca Bagni.