VOL. 7 - SPECIAL ISSUE
(2026)

Journal of International Criminal Law

Online Scientific Review

Special Issue
EU-GLOBACT HANDBOOK

EUROCRIMES

EDITED BY
Heybatollah Najandimanesh
Anna Oriolo

ISSN: 2717-1914

www.jiclonline.org

EU-GLOBACT HANDBOOK

EUROCRIMES

A Q&A COMPENDIUM AND STRUCTURAL FRAMEWORKS ON OFFENCES UNDER ARTICLE 83 TFEU

This JICL Special Issue constitutes one of the scientific products the Jean Monnet Module (2023-2026) *Transnational Crime and EU Law: Towards Global Action against Cross-Border Threats to Common Security, Rule of Law, and Human Rights* (EU-GLOBACT) – (Coordinator: Prof. Dr. Anna Oriolo).

Co-funded by the European Union

Project funded by European Commission Erasmus + Programme – Jean Monnet Action Project number 101126599. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents
Volume 7 – Special Issue

Board of Editors

OVERVIEW

The Journal of International Criminal Law (*JICL)* is a scientific, online, peer-reviewed journal, first edited in 2020 by Prof. Dr. Heybatollah Najandimanesh, mainly focusing on international criminal law issues.

Since 2023 JICL has been co-managed by Prof. Dr. Anna Oriolo as General Editor and published semiannually in collaboration with the International and European Criminal Law Observatory (IECLO) staff.

JICL Boards are powered by academics, scholars and higher education experts from a variety of colleges, universities, and institutions from all over the world, active in the fields of criminal law and criminal justice at the international, regional, and national level.

The aims of the JICL, *inter alia*, are as follow:

- to promote international peace and justice through scientific research and publications;
- to foster study of international criminal law in a spirit of partnership and cooperation with the researchers from different countries;
- to encourage multi-perspectives of international criminal law; and
- to support young researchers to study and disseminate international criminal law.

Due to the serious interdependence among political sciences, philosophy, criminal law, criminology, ethics and human rights, the scopes of JICL are focused on international criminal law but not limited to it. In particular, the Journal welcomes high-quality submissions of manuscripts, essays, editorial comments, current developments, and book reviews by scholars and practitioners from around the world addressing both traditional and emerging themes, topics such as

- the substantive and procedural aspects of international criminal law;
- the jurisprudence of international criminal courts/tribunals;
- mutual effects of public international law, international relations, and international criminal law;
- relevant case-law from national criminal jurisdictions;
- criminal law and international human rights;
- European Union or EU criminal law (which includes financial violations and transnational crimes);
- domestic policy that affects international criminal law and international criminal justice;
- new technologies and international criminal justice;
- different country-specific approaches toward international criminal law and international criminal justice;
- historical accounts that address the international, regional, and national levels; and
- holistic research that makes use of political science, sociology, criminology, philosophy of law, ethics, and other disciplines that can inform the knowledge basis for scholarly dialogue.

The dynamic evolution of international criminal law, as an area that intersects various branches and levels of law and other disciplines, requires careful examination and interpretation. The need to scrutinize the origins, nature, and purpose of international criminal law is also evident in the light of its interdisciplinary characteristics. International criminal law norms and practices are shaped by various factors that further challenge any claims about the law's distinctiveness. The crime vocabulary too may reflect interdisciplinary synergies that draw on domains that often have been separated from law, according to legal doctrine. Talk about "ecocide" is just one example of such a trend that necessitates a rigorous analysis of law *per se* as well as open-minded assessment informed by other sources, *e.g.*, political science, philosophy, and ethics. Yet other emerging developments concern international criminal justice, especially through innovative contributions to enforcement strategies and restorative justice.

The tensions that arise from a description of preferences and priorities made it appropriate to create, improve and disseminate the JICL as a platform for research and dialogue across different cultures, in particular, as a consequence of the United Nations push for universal imperatives, *e.g.*, the fight against impunity for crimes of global concern (core international crimes, transboundary crimes, and transnational organized crimes).

COPYRIGHT AND LICENSING

Money Laundering

by Emanuele Sorgente[*]

SUMMARY: I. Why Does Money Laundering Represent an Inherently Transversal Global Challenge? – II. What Are the Three Structural Stages Characterizing the International Laundering Cycle? – III. What Link Exists Between Money Laundering and Terrorist Financing in The International System? – IV. What Core Strategies Drive the Evolution of European Anti-Money Laundering Directives? – V. In What Way Does Money Laundering Fall Within PIF Offenses Under the Competence of the EPPO? – VI. What Is Meant By "Green Money Laundering" Under the Protecting Framework of Directive 2024/1203? – VII. What Criminal and Prevention Norms Define the Offense of Money Laundering Under Domestic Law? – VIII. How Is the Autonomy of Self-Laundering Structured in Light of The Jurisprudence of the CJEU? – IX. How Does Financial Masking Adapt to Blockchain Systems and Decentralized Cryptocurrencies?

KEY FINDINGS: Global profile, Transversality, and money dirtying; Multilevel integration and the Palermo turning point; The new "AML Package" and the centralization of AMLA; Autonomy of self-laundering and PIF protection of EPPO; The new frontier of "green money laundering" in cyberspace.

I. Why Does Money Laundering Represent an Inherently Transversal Global Challenge?

Money laundering is a criminal phenomenon that, until the 1980s, was entirely unknown to traditional penal sciences. Today, however, it represents one of the main *global challenges*, prompting the International Community (or, more precisely, the United Nations) and major institutions, such as the European Union, to adopt a regulatory framework aimed at countering it. This regulatory framework, however, exhibits significant fragmentation at the geographical level. The processes of market financialisation and the dematerialisation of goods have caused a proliferation of new financial instruments and rapid payment techniques. These very digital and liquid instruments are systematically employed by organised crime to launder and increase their massive capital. According to estimates by the Financial Action Task Force (FATF) and the UN, money laundering annually generates approximately 2-5% of global GDP, a macroeconomic figure ranging between 800 and 2,000 billion dollars. One of the main peculiarities characterizing money laundering is its inherently "transversal" nature, which is reflected in the indissoluble link connecting it to other serious crimes, such as drug trafficking, human trafficking, migrant smuggling, administrative corruption, cybercrime, arms trafficking, and terrorism – where it would be more appropriate to speak

[*] Member of the Secretariat of the International & European Criminal Law Observatory (IECLO), University of Salerno, Italy.

JICL (Vol. 7 – Issue 1 – 2026), pp. 66-77
ISSN 2717-1914

of "Money Dirtying", since the funds used to finance it very often have a completely lawful origin. This list does not constitute a *numerus clausus*, as money laundering is an extremely versatile crime. The international legal order has adopted a multilevel approach to counter the phenomenon, combining rules and monitoring bodies, given the clear awareness of the ineffectiveness of purely state-centric repressive instruments.

REFERENCES

UNTOC, 2000, Art. 6

The first step toward harmonization occurred in 1989 with the non-binding "Declaration of Principles" by the Basel Committee (G10 States). At the conventional level, the 1988 UN Vienna Convention regulated money laundering indirectly and as a secondary crime linked exclusively to narcotics. Operating as a counterweight were the FATF 40 Recommendations of 1990 (extended in 2001 to terrorist financing through 9 Special Recommendations), endowed with strong *moral suasion*. The true regulatory turning point occurred with the **United Nations Convention against Transnational Organized Crime of 2000 (Palermo Convention)**, which overcomes the sectoral approach and broadens the scope of **predicate offenses**. It introduced Art. 7 (measures for banking institutions) and **Art. 6** (Criminalization of laundering), which urges States to criminalize the conversion, transfer, and concealment of property knowing that such property constitutes proceeds of crime (Art. 6, para. 1, let. a and b), including predicate offenses committed both within and outside the jurisdiction of the State Party (Art. 6, para. 2, let. b and c).

II. What Are the Three Structural Stages Characterizing the International Laundering Cycle?

Regardless of the different international definitions (the 1988 Vienna Convention anchored to drugs, the 2000 Palermo Convention extended to serious crimes, the Council of Europe Strasbourg Convention aimed at masking, and the European Union focused on concealing the illicit origin), money laundering generally comprises **three stages: placement, layering, and integration**. Faced with a financial landscape transformed by the digital transition and the presence of offshore countries, money launderers resort to complex procedures favored by financial disintermediation and the professionalization of the activity, which manifests in the emergence of **White-Collar Crimes**. These are offences committed by individuals possessing a high social status in the course of their occupation (fraud, embezzlement, insider trading, money laundering), aimed at obtaining an illicit gain or avoiding financial losses, complicating tracking through elaborate schemes. Organised crime syndicates enlist qualified intermediaries operating in the financial sector, who act on both an active level (facilitating the distorted use of complex financial products and credit provision) and a passive level (providing tools for concealing illicit funds).

FOCUS

The Three Stages of Laundering and Art Market Components

- **Placement:** Illicit proceeds are introduced into the domestic or international market through institutions or intermediaries, or via direct asset purchases. Typical techniques include *Smurfing* (the strategic subdivision of cash into small amounts deposited into numerous bank accounts by multiple strawmen), mixing funds with legitimate commercial cash flows, deposits at non-bank financial institutions, physical cash smuggling across borders, and purchasing bearer negotiable instruments.
- **Layering:** Illicit wealth is layered across the market through multiple transactions to sever the link with the predicate offense. It includes multiple rapid electronic transfers (*wire transfers*), shell company and trust operations in tax havens, complex financial transactions in derivatives and shares through offshore intermediaries, purchasing and selling luxury assets (real estate, luxury cars, artworks), gambling networks, and *Loan Back* mechanisms (fictitious loan contracts between related foreign companies to justify the repatriation of funds).
- **Integration:** Consists of the final reintroduction of the fully "washed" proceeds into the legitimate economic and industrial circuits, materializing in the purchase of prestigious real estate, investments in legitimate commercial and financial activities, or the creation of foundations and non-profit organizations used as a shield.
- **The Vulnerability of the Art Market:** Represents a sector highly exposed to infiltration and money laundering risks, since artworks reach exorbitant prices devoid of an objective baseline (making it easy to artificially inflate or deflate the value), transactions often occur anonymously through shell companies, and the works are easily transportable across international borders. To mitigate this exposure, the European Union has imposed stringent *due diligence* and suspicious transaction reporting obligations on galleries and auction houses.

III. What Link Exists Between Money Laundering and Terrorist Financing in the International System?

While the fight against money laundering was initially focused on illicit proceeds from traditional organized crime, the sophistication of the global terrorist threat has made the dangerous synergy between the two crimes evident. Money laundering can operate as a logistic means to finance eversive activities: the two offences pursue different ends but converge methodologically, sharing the need to conceal and move financial flows. The FATF Special Recommendations (specifically 5, 6, and 8) require countries to criminalize terrorist financing in line with the 1999 New York Convention (under which it became an autonomous crime distinct from terrorism), to implement targeted financial sanctions, and to review regulations governing non-profit organizations (NGOs) to prevent their abuse. At the regional level, the Council of Europe adopted two primary sources: the **1990 Strasbourg Convention** (aimed at harmonizing legislations and rendering the fight effective through mechanisms of investigation, search, seizure, and confiscation of proceeds) and the **2005 Warsaw Convention** (Convention on Laundering and Terrorist Financing).

REFERENCES

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention), 2005, and IFTS Channels

The Warsaw Convention stems from the realization that terrorism can be fueled by funds of not only illicit but also lawful origin (**"Money Dirtying" – Art. 5**), imposing an obligation to criminalize the provision or collection of funds when accompanied by the intention or knowledge that they will be used to commit terrorist offenses. **Art. 7** also provides for corporate liability for offenses committed for their benefit. While Strasbourg focuses on definitional profiles and broadening the scope of proceeds, Warsaw focuses specifically on the material act of provision or collection; banking *due diligence* and suspicious transaction reporting (STR) remain instrumental. For eversive purposes, terrorist groups heavily rely on **IFTS (Informal Funds Transfer Systems)**: these are alternative mechanisms based on mutual trust between independent agents or brokers (such as the clandestine *Hawala* network), operating entirely outside the traditional banking system. Originally emerging for lawful purposes like migrant remittances and trade, their lack of transparency and the absence of centralized accounting ledgers render them ideal for money laundering and terrorism financing.

Faced with these operational requirements, the Council of Europe established the **Moneyval** Committee of experts, tasked with a plurality of peer-review and audit functions:

- Assessing the legislative compliance of its Member States with international standards and the FATF 40 Recommendations.
- Evaluating the effectiveness and material application of these standards in the real-world context.
- Identifying in real time new trends and technical methods of money laundering and eversive financing.
- Drafting detailed periodic monitoring reports to indicate to States the administrative or judicial areas requiring urgent improvements.
- Strengthening international cooperation and operational ties with the FATF, the International Monetary Fund (IMF), the European Union, and the UN.
- *Detailed study suggestion:* Study the configuration of general intent (*dolo generico*) and specific intent (*dolo specifico*) in the crime of terrorist financing, analyzing how the conduct is perfected independently of the actual material execution of the primary terrorist attack.

IV. What Core Strategies Drive the Evolution of European Anti-Money Laundering Directives?

Money laundering represents a severe threat to the economic and financial stability of the European Union, capable of harming the Union's financial interests and provoking distortion of free competition (Art. 83 TFEU). The EU has adopted specific counter-strategies translated into an evolution of secondary law subject to constant institutional updates to face new challenges posed by financial disintermediation:

- **Directive 1991/308/EEC (First AML Directive):** The first milestone at the community level establishing the legal notions of credit and financial institution, borrowing the definition of laundering from the 1988 Vienna Convention and receiving the original FATF Recommendations. *(Repealed)*.

- **Directive 2001/97/EC (Second AML Directive):** Concerning prevention of the use of the financial system for the purpose of money laundering, it brought substantial amendments and extended the catalogue of predicate offenses beyond drug trafficking. *(Repealed)*.
- **Directive 2005/60/EC (Third AML Directive):** Aimed at preventing the use of financial and non-financial sectors, introducing measures to establish the true identity of clients, report suspicious transactions, and establish internal compliance presidios, supplemented by Directive 2006/70/EC regarding **PEP (*Politically Exposed Persons*)**. *(Repealed)*.
- **Directive 2015/849/EU (Fourth AML Directive):** Succeeded the previous 2005 framework to eliminate interpretative ambiguities and improve the internal consistency of AML/CFT rules. It significantly reinforces transparency regarding the identification of clients and **beneficial owners** of companies and trusts, requiring this information to be stored by States in centralized registries. It provides a coordinated European policy for dealing with high-risk uncooperative third countries and strengthens transnational cooperation between **Financial Intelligence Units (FIUs)** for the reporting of suspicious cases. It was amended by Directives 2018/843 (Fifth AML Directive), 2019/758, and **Regulation (EU) 2023/1113**, which, to counter the illicit use of cryptographic technologies, included all **CASPs (*Crypto-Asset Service Providers*)** in the definition of "financial institutions", subjecting wallet providers to *due diligence* obligations. *(Will be repealed as of June 1, 2027, by Directive 2024/1640)*.

REFERENCES

The European Commission's New "Anti-Money Laundering Package", 2024

In May 2020, the European Commission, through a Communication (C 2020/2800), proposed an ambitious Action Plan structured around six pillars for an integrated prevention policy. These objectives were recently realized with the publication in the Official Journal, on June 19, 2024, of the historic **Anti-Money Laundering Package (AML Package)**, which consists of:

- **Regulation (EU) 2024/1624 (Single RuleBook):** Regulates contrast within the private sector by introducing directly applicable rules on *due diligence*, *crowdfunding*, *crypto-assets*, and beneficial owners. It broadens the category of obliged entities to virtual currency exchange providers and traders of luxury and cultural goods whenever the transaction **exceeds the threshold of 10,000 euros**, fixing a **maximum European limit for cash payments at 10,000 euros**. It will apply from July 10, 2027 (from July 10, 2029, for football agents and professional football clubs).
- **Sixth Anti-Money Laundering Directive (Directive EU 2024/1640):** Provides rules on the maintenance and interconnection of beneficial ownership registries and effective supervision. It introduces the mandatory appointment of a *Fundamental Rights Officer* to ensure respect for fundamental rights and data protection within national FIU operations. It must be transposed by Member States by July 10, 2027.
- **Regulation (EU) 2024/1620 (Establishment of the AMLA):** Formally establishes the new central **Anti-Money Laundering Authority (AMLA)**, with its official seat located in **Frankfurt**, Germany.

V. In What Way Does Money Laundering Fall Within PIF Offenses Under the Competence of the EPPO?

Money laundering is classified among the **"PIF offences"**, meaning those crimes that harm the financial interests of the European Union, on the same dogmatic level as corruption, aggravated fraud, and misappropriation of public funds. These financial interests constitute the core material competence of the **EPPO (European Public Prosecutor's Office)**, established under Regulation (EU) 2017/1939. The EPPO's jurisdiction qualifies as a priority but concurrent competence with national judicial authorities, activating whenever the Luxembourg-based prosecution office decides to exercise its right of evocation over a case. The EPPO is also competent for offenses relating to participation in a transnational criminal organization if the strategic objective of the syndicate is to commit a PIF offense, provided that the conduct was committed, in whole or in part, in the territory of one or more participating EU Member States, by a national of a participating Member State, or by an official or agent of the European Union institutions.

REFERENCES

The "PIF" Directive (EU) 1371, 2017, and Inter-Agency Operability

Directive (EU) 2017/1371 defined the scope of the notion of "fraud and damage to the financial interests of the EU", identifying the offenses to be prosecuted within the common market. The *ratione materiae* scope extends to connected offenses, explicitly establishing that **the EPPO is competent for money laundering only if the laundered money originates from one of the predicate offenses that harm the financial interests of the EU** (e.g., fraud on regional development funds, CAP agricultural subsidies, or cross-border VAT fraud). The EPPO has strengthened the fight against cross-border laundering and holds the direct power to order the provisional seizure and mandatory confiscation of assets and illicit proceeds. The European Public Prosecutor's activity is integrated within an advanced institutional architecture based on synergy with other European agencies with complementary competencies:

- **The European Anti-Fraud Office (OLAF):** Conducts investigations exclusively on an administrative and non-criminal level regarding fraud against the EU budget, corruption, and professional misconduct within the institutions, providing the EPPO with all the results of its audits and tracking of community funds.
- **The European Union Agency for Law Enforcement Cooperation (Europol):** Facilitates the rapid and secure exchange of information between Member States' police forces via its network of liaison officers (Art. 87 TFEU). It performs macro-criminal analysis and data collection to identify money laundering models, providing specialized expertise to counter cryptocurrency use and *cyber-laundering*.
- **The EPPO (European Public Prosecutor's Office):** Utilizes the administrative findings of OLAF and the criminal analyses of Europol to independently exercise criminal action and request the freezing and seizure of white-collar assets before national courts.

VI. What Is Meant By "Green Money Laundering" Under the Protecting Framework of Directive 2024/1203?

The expression **"Green Money Laundering"** identifies the criminal convergence between ecocide and the laundering of illicit wealth originating from environmental crimes, an area that the FATF, within a 2020 strategic report on the financial flows of

illegal wildlife trade, elevated to a global investigative priority. Environmental crimes constitute an extremely lucrative and low-risk macro-economic activity, covering conduct ranging from illegal logging and wild mining to the **illegal trafficking of toxic and hazardous waste**. The illicit proceeds generated by these eco-offenses must be "cleaned" through banking circuits to be freely reinvested, translating into massive asymmetric damage that strikes not only the transparency of the global financial system but irreversibly devastates ecosystems, biodiversity, and planetary sustainability. Criminals rely on cash-intensive sectors and implement complex commercial frauds, utilizing **shell companies located in offshore financial centers or fictitious companies (*buffer* entities)** to conceal payments and simulate legitimate contracts and trade.
Widespread techniques include commercial fraud based on falsifying customs documentation for importing and exporting goods (e.g., timber origin certificates) and creating false invoicing for non-existent transactions to justify capital movements across borders. The most complex element for law enforcement lies in the systematic **physical mixing and blending of lawful and illicit goods** (e.g., mixing hazardous chemical waste into regular urban trash shipments), making it extremely difficult to detect criminal profiles within apparently clean operations, aided by the massive overall volume of global transactions in this sector. During the crucial **layering stage**, a fundamental contribution is provided by professionals and white-collar facilitators – such as accountants, surveyors, and corrupt lawyers. In the specific sector of illegal waste trafficking, organized groups use companies registered to complicit strawmen, formally equipped with all regular administrative-environmental permits, using them as washing machines to blend dirty cash flows with the legitimate commercial revenues of the firm.

FOCUS

The Camorra Waste Trafficking of the Milan Case, April 2025, and Directive (EU) 1203, 2024

The severity of the phenomenon is illustrated by the investigation conducted in **April 2025 by the Guardia di Finanza, coordinated by the Public Prosecutor's Office of Milan**, which dismantled a massive illegal waste trafficking operation orchestrated by a criminal organization with deep roots in the **Camorra**, culminating in the preventive seizure of **92 million euros** [Europol]. The syndicate specialized in the illicit trafficking of metallic waste (copper and aluminum) supplied to industrial firms in Northern Italy. To mask the lawful nature of the exchange, a complex system of false invoicing was activated involving more than **51 shell companies (*cartiere*)**, registering non-existent operations for an astronomical value exceeding **320 million euros**. The proceeds were rapidly transferred to foreign bank accounts in an attempt to sever the causal link with the predicate offense and perpetrate self-laundering, proving that waste trafficking fuels transnational financial circuits.
Faced with this awareness, the European Union adopted the new **Directive (EU) 2024/1203 on the protection of the environment through criminal law**, whose **Recital (28)** explicitly mandates that environmental criminal proceedings must not treat the matter in isolation. Instead, they must address in an integrated manner the corruption, money laundering, cybercrime, and documentary fraud orchestrated by organized crime groups to maximize profits or avoid expenses, given the devastating impact on nature and human health.

VII. What Criminal and Prevention Norms Define the Offense of Money Laundering Under Domestic Law ?

The Italian criminal and administrative order has progressively conformed to the rigid standards of sanctions standardization imposed by international and European sources. A first fundamental step occurred with **Decree-Law March 21, 1978, no. 59** (converted by Law no. 191/1978), which introduced for the first time into the penal system the independent crime of money laundering by inserting **Art. 648-*bis* within the Criminal Code**. This offense was subsequently redefined and structured in its current precetive form by **Law August 9, 1993, no. 328**, concerning the "Ratification and execution of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, done at Strasbourg on November 8, 1990". Through **Legislative Decree no. 153/1997**, Italy transposed the first Community AML Directive 91/308/EEC, introducing the figure of the Italian Foreign Exchange Office (UIC) and broadening administrative obligations of customer identification and reporting. The fundamental pillar of reference regarding administrative prevention is currently **Legislative Decree November 21, 2007, no. 231**, which transposed subsequent European Directives, working alongside Legislative Decree no. 109/2007 for the economic block of terrorist flows. **Art. 2** of Legislative Decree 231/2007 contains an all-encompassing notion of money laundering (Para. 4 and Para. 5), extending its illicitness even if the predicate activities took place outside national borders, and of terrorist financing (Para. 6), defined as any activity directed at providing or collecting funds usable for eversive conduct regardless of their actual material use.

REFERENCES

Italian Criminal Code, Art. 648-*bis* and Art. 648-*ter*

Art. 648-*bis* (Money Laundering): "Outside the cases of complicity in the crime, anyone who replaces or transfers money, assets or other utility derived from a crime; or performs in relation to them other operations, in such a way as to obstruct the identification of their criminal origin, shall be punished with imprisonment from four to twelve years and with a fine from 5,000 to 25,000 euros".

Art. 648-*ter* (Self-Laundering): For a long time, this phenomenon was considered non-punishable, qualified by traditional doctrine as a mere *post-factum* of the predicate offense; it was introduced into the criminal code by **Law December 15, 2014, no. 186**. The article establishes: "The penalty of imprisonment from two to eight years and a fine from 5,000 to 25,000 euros applies to anyone who, having committed or concurred in committing a crime, employs, replaces, transfers, in economic, financial, entrepreneurial or speculative activities, the money, assets or other utilities derived from the commission of such crime, in such a way as to concretely obstruct the identification of their criminal origin".

A cornerstone of the Italian system is the **Risk-Based Approach**, which must guide the behavior of obliged entities, requiring a close strategy between private economic operators, independent administrative authorities (**UIF**), and investigative bodies (**Guardia di Finanza**). The intensity of *due diligence* measures is proportional to the concrete risks identified based on a periodic assessment of systemic vulnerabilities, exposed sectors, and audit reports drafted by the European Commission. The order mandates compliance with **customer due diligence (KYC)** and ten-year document conservation duties. The pool of obliged entities has been massively extended: it no longer comprises only banks, but includes professionals (lawyers, notaries, accountants), statutory auditors, and non-financial operators (art dealers, auction houses). In full alignment with the **2026** scenario dictated by the European Single Rulebook, **CASPs (*Crypto-Asset Service Providers*)** are fully included. Another structural measure is the legal limitation on cash use, whose **domestic maximum threshold is set at 5,000 euros**.

VIII. How Is the Autonomy of Self-Laundering Structured in Light of The Jurisprudence of the CJEU?

The Bank of Italy, established historically in 1893 and becoming in 1926 the sole institution authorized to issue banknotes and exercise banking supervision, operates today as the central bank of the Italian Republic and is an integral part of the Eurosystem and the ECB, ensuring monetary and financial stability. With specific reference to money laundering, the Bank of Italy, through the **Anti-Money Laundering Supervision and Regulation Unit**, plays a fundamental role: it actively participates in the sessions of the FATF, the Basel Committee, and the **EBA (European Banking Authority)**; it monitors international and domestic regulatory production, maintaining advisory relationships with the Government, Parliament, and other sector supervisors (Consob, Ivass); it develops advanced analysis and evaluation methodologies in AML/CFT; it conducts on-site inspections and off-site audits of supervised intermediaries; and it cooperates by exchanging data and confidential info with the **UIF** and the Guardia di Finanza. Supervision of the credit system is indispensable for ensuring market integrity: the infiltration of illicit capital into the economic fabric constitutes a serious threat that undermines the solidity of credit intermediaries. The involvement of a bank in laundering operations, even if completely involuntary due to control failures, produces severe systemic risks: organized crime can condition corporate management, bending it to illicit interests; it causes a dramatic loss of confidence on a reputational level by clients; and it induces a progressive compromise of the intermediary's financial stability.

FOCUS

Supervisory Mechanisms and Inspection Tools of the Bank of Italy

The Anti-Money Laundering function configures as a transversal capability integrating institutional supervisory activity, expressing itself through specific operational modules:

- **Evaluation of Authorizations:** In granting authorizations for starting new banking activities or extraordinary corporate operations, it carefully evaluates the anti-money laundering framework; in case of critical anomalies, the authorization can be conditional on corrective measures or denied.
- **Application of the Risk-Based Approach:** Modulates prevention action in a via proportional manner to the concrete risk of the specific case, considering that the risk associated with a private citizen is fundamentally different from that of a complex shell company, taking as baseline parameters the subject, the object, and the geographical operational context.
- **Customer Due Diligence (Know Your Customer - KYC):** Presides over the development of procedures aimed at creating and deepening the economic profile of the client, essential for evaluating transaction consistency and detecting anomalies.
- **Single Automated Archive (*Archivio Unico Informatico - AUI*):** Monitors the correct maintenance of the central secured digital registry where intermediaries must obligatorily log relationships and relevant transactions above the threshold.
- **Supervisory Inspections and Sanctions:** Conducts on-site audits or cartolar document verifications, from which arise administrative pecuniary penalties and direct criminal referrals to the penal judicial authority.
- **UIF *Presidio*:** Established autonomously and independently within the Bank of Italy is the **Financial Intelligence Unit (*Unità di Informazione Finanziaria - UIF*)**, the body responsible for receiving, analyzing, and transmitting **Suspicious Transaction Reports (STRs / SOS)** to the Anti-Mafia Prosecution Office, also tasked with drafting anomaly indicators and behavioral models to support obliged private operators.

IX. How Does Financial Masking Adapt to Blockchain Systems and Decentralized Cryptocurrencies?

In the contemporary era, characterized by a constant and pervasive digital transition, the crime of money laundering has stably settled within the dematerialized infrastructures of cyberspace, drawing massive eversive momentum from emerging technologies. The speed and intrinsic flexibility with which laundering methods adapt to technological and computer progress threaten to render traditional analog-banking contrast strategies increasingly ineffective, forcing doctrine and international legislators to constantly extend the scope of predicate offenses. Under a penal dogmatic and cyber-forensics profile, there is an indissoluble systemic interconnection linking money laundering to the macro-category of **Cybercrime**, with which it shares both the virtual operating environment and computer methodologies. In this context, **crypto-assets** perform a fundamental logistical role due to the structural absence of centralized institutional counterparts (such as credit intermediaries) and the pseudo-anonymous nature governing the distributed ledgers of the blockchain. Cryptocurrencies facilitate instantaneous cross-border financial transfers, operating entirely outside traditional banking supervision networks, making them highly attractive to organized crime and feeding complex, elaborate laundering schemes.

FOCUS

Cyber-Laundering Techniques and Forensic Methodologies

- **Cryptocurrency Mixers / Tumblers:** Computer platforms and protocols designed for privacy protection, they are used illicitly to merge, mix, and fragment cryptocurrency flows from hundreds of different wallets and separate predicate crimes, redistributing the funds to obscure the logical chain of the blockchain and mask the original source.
- **Peel Chains:** An automated algorithmic procedure that makes accounting reconstruction of the flow highly complex; a large mass of dirty cryptocurrency is progressively "peeled" and atomized through a dense cascade of small automated transactions that elude computer security alert thresholds, flowing into clean wallets.
- **Chain Hopping:** This methodology aims at obscuring the origin of the virtual flow through the rapid and constant exchange of different *digital assets*. Funds do not remain anchored to a single cryptocurrency but are shifted abruptly from one chain to another by exchanging them for different virtual currencies (e.g., from Bitcoin to Monero or Ethereum) across multiple digital exchange platforms (*Exchanges*), disorienting transnational tracking devices.
- **The New Frontier of NFTs and Artificial Intelligence:** In recent years, complex criminal modules centered on the speculative use of **NFTs (*Non-Fungible Tokens*)** and privacy-centric blockchain networks have emerged. To counter this, law enforcement relies on sophisticated algorithms and **Artificial Intelligence applied to *blockchain forensics*** to map flows and identify anomalous commercial *patterns*, intercepting wallet connections with known illicit addresses (such as *Darknet Markets* or terrorist nodes), de-anonymizing operations through *clustering* techniques aimed at grouping addresses belonging to the same source.
- **Biometric Adequate Verification:** Exchange platforms (CASPs), in line with the dictates of Regulation (EU) 2023/1113, have implemented rigorous verification procedures to prevent anonymity, requiring valid documents for individuals and company registration certificates for legal entities, integrating controls with public databases and utilizing **live selfie technologies for instantaneous biometric client verification**, constantly monitoring transactions to forward suspicious reports directly to the UIF.

FOCUS

The Ponzi Scheme of the Plus Token Crypto Fraud, 2019

The operation of *cyber-laundering* on a massive scale is highlighted by the colossal **Plus Token case**. The platform presented itself on the Asian market as an innovative cryptocurrency wallet, attracting investors with the false promise of high fixed monthly dividends conditioned on depositing first-tier assets like Bitcoin and Ethereum. Users were also promised substancial economic rewards for the constant recruitment of new members, a structural dynamic reflecting the classic traits of a **Ponzi Scheme** and a pyramid fraud. The credibility of the platform relied on strategic affiliations with public figures and accredited blockchain and trading experts. In June 2019, the application blocked withdrawals and stopped functioning, generating widespread panic. The operators, after fraudulently embezzling billions of dollars, activated the *layering* phase, attempting to clean the wealth by shifting massive quantities of cryptocurrency to smaller, less regulated offshore exchanges, utilizing *chain hopping* to swap assets and enlisting *mixer* services to blend funds. International law enforcement agencies, coordinated with forensic protocols, managed to track and order the **seizure of massive quantities of cryptocurrencies**, while encountering massive procedural and logistical difficulties regarding the storage, liquidation, and forced disposal of the confiscated digital assets, confirming the severe technological vulnerabilities to which the contemporary financial market is exposed.

CASE STUDY

The Italian Supreme Court of Cassation's Position

Domestic jurisprudence of legitimacy has conformed to these technological evolutions, extending criteria of penal punishability to offenses committed abroad and to telematics frauds:

- **Court of Cassation, Judgment No. 23679 (2020) (Transnational Jurisdiction):** The judges of legitimacy secured the international reach of the offense, ruling that: "It is then peaceful in the jurisprudence of this Court of legitimacy that the predicate offense of money laundering can also be committed abroad", validating the transnational nature of the case.
- **Court of Cassation, Judgment No. 19125 (2023) (Cyber-Laundering and Money Mules):** The Supreme Court addressed telematics frauds, ruling that: "In particular, this Court has stated that the conduct of those who, without having competed in the predicate offense, make their prepaid card or bank account available to obstruct the criminal origin of the sums derived by others through a cyber-fraud integrates the crime of money laundering", penalizing the so-called **"Money Mules"** and digital facilitators who lend their credentials for the placement phase.

X. Key Findings

The dogmatic, historical, regulatory, and jurisprudential analysis carried out within this work leads to the delineation of **five fundamental findings**:

- **Global Profile, Transversality, and Money Dirtying:** Money laundering constitutes an asymmetric global threat draining between **2% and 5% of global GDP** (up to 2,000 billion dollars a year). Its profile is characterized by a strong cross-disciplinarity, operating as a consequential offense downstream of all major *Eurocrimes* ex Art. 83 TFEU; in the field of terrorism, doctrine prefers the expression **"Money Dirtying"**, since the starting funds often have a lawful origin and are subsequently diverted by the eversive destination of use, transiting through the opacity of informal **IFTS systems (the clandestine *Hawala* network)**.

- **Multilevel Integration and the Palermo Turning Point:** The prevention architecture rests on a multilevel model connecting the *soft law* sources of the FATF (40 Recommendations) with the binding treaties of the United Nations. **Art. 6 of the 2000 Palermo Convention** constitutes the cornerstone of the matter, forcing States to criminalize the three stages of the laundering cycle (**placement, layering, and integration**) and extending predicate offenses (*predicate offenses*) to crimes committed outside the national jurisdiction, overcoming the barriers of bank secrecy.
- **The New "AML Package" and the Centralization of AMLA:** The European Union has revolutionized its legal framework through the publication of the "Anti-Money Laundering Package" on June 19, 2024. This corpus introduces the *Single Rulebook* (Regulation EU 2024/1624) – which fixes the maximum European limit for cash payments at 10,000 euros and extends *due diligence* obligations to **crypto-asset markets (Regulation EU 2023/1113)** and the professional football sector from 2029 – the Sixth Directive, and the establishment of **AMLA in Frankfurt**, a central authority endowed with direct supervisory and sanctioning powers over high-risk financial institutions.
- **Autonomy of Self-Laundering and PIF Protection of EPPO:** Under a dogmatic profile, the historic **judgment of the CJEU of September 2, 2021 (case C-790/19)** sanctioned the full compatibility of self-laundering with European law, confirming the structural autonomy of the conduct with respect to the predicate offense and the non-violation of the *ne bis in idem* principle. Laundering is also classified among **"PIF offenses"** under Directive (EU) 2017/1371, rooting the material competence of the **European Public Prosecutor's Office (EPPO)** for the exercise of criminal action and asset confiscation, in constant synergy with the administrative investigations of **OLAF** and the criminal analyses of **Europol**.
- **The New Frontier of "Green Money Laundering" in Cyberspace:** The infiltration of white-collar professionals into ecological markets has given rise to the phenomenon of green laundering, aimed at cleaning the proceeds of illegal waste trafficking and logging through offshore shell companies and commercial frauds, in full implementation of **Recital (28) of the new Directive (EU) 2024/1203 on the protection of the environment through criminal law**, and modern channels of *cyber-laundering* and telematics frauds (*money mules*), striking the complex pyramid schemes emerged in the **2019 Plus Token case** through tracking techniques and algorithms of de-anonymization of forensic blockchain.