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).


*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

# Foreword

*by Anna Oriolo*[*]

This JICL Special Issue constitutes one of the scientific products of the Jean Monnet Course EU-GLOBACT (*Transnational Crime and EU Law: Towards Global Action against Cross-border Threats to common security, rule of law and human rights*), co-funded by the European Commission (2023-2026).

The EU-GLOBACT Project has aimed to promote excellence in teaching and research within European Union (EU) legal studies at the University of Salerno and, specifically, within the Department of Legal Sciences, offering a free, highly specialized, and interdisciplinary course focused on the emerging global policy of the EU in the fight against transnational crime, relevant both to the future professional careers of graduates and to the advanced training of legal and political practitioners. As such, it has intended to foster shared research and an exchange of ideas to identify solutions and examples of best practices in combating transnational crime that could be replicated by all States (both European and non-European), as well as to contribute to the development of legislation and policies in line with EU values and principles.

To achieve these goals, EU-GLOBACT has combined teaching projects, research initiatives, and dissemination activities, adopting a multidisciplinary, gender-equal, and non-discriminatory approach.

From a methodological standpoint, EU-GLOBACT activities have blended traditional (legal) instruction with the "hands-on" approach typical of so-called *law clinics*, namely the application of legal knowledge to concrete cases. This objective was achieved by conducting teaching, research, and dissemination initiatives under the umbrella of the *International & European Criminal Law Observatory* (IECLO), which I founded and have directed at the Department of Legal Sciences since 2022.

Although the transnational crimes affecting the contemporary landscape are multifaceted and diverse, this Special Issue is specifically dedicated to and perimetrated around the Eurocrimes listed under Article 83, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU). However, while maintaining its distinct "EU-centered" thematic autonomy, the work avoids a rigidly isolated perspective. To fully integrate the European Union into the global geopolitical context and highlight its role as a global actor in the fight against transnational crime (which constitutes the core purpose and objective of EU-GLOBACT), the answers systematically connect the European dimension with the broader framework of international and treaty law (UN, Council of Europe, NATO).

This multilevel architecture is complemented by an analysis of the national perspective (focusing in particular on Italy as the seat of our reference scientific and research institutions), which allows for an assessment of the material impact and effectiveness of domestic techniques for transposing supranational sources into the national legal order.

[*] Associate Professor of International Law, University of Salerno; IECLO Director; EU-GLOBACT Scientific Coordinator; JICL General Editor.

The development and editorial care of this specific tool, which is designed to serve as an informative and educational support, have been conducted by the members of the IECLO Secretariat, in particular by Francesco Foccillo to whom I extend my special and heartfelt thanks. As for the Special Issue contents, the individual modules host the contributions of Luisanna Savino (International Terrorism), Orsola Ilenia Conte (Human Trafficking and Sexual Exploitation of Women and Minors), Emanuela Coppola and Fernanda Masullo (Illicit Drug Trafficking), Francesco Foccillo (Counterfeiting of Means of Payment and Violation of Union Restrictive Measures), Emanuele Sorgente (Money Laundering), Christian Fausto Santoriello (Corruption), Teresa D'Aniello (Computer Crime), and Alessandra Giordano and Miriana Greco (Transnational Organized Crime).

The study of an intrinsically complex subject, such as the origins and development of transnational crime and the strategies to counter it, requires cutting-edge analytical tools capable of facilitating student learning and professional training. In this perspective, this JICL Special Issue has been structured according to the innovative *Question & Answer Handbook* model. The architecture of this *Handbook* is reinforced by specialized legal, jurisprudential, and conceptual briefs designed to facilitate the immediate assimilation of definitions, cooperation frameworks, and European and international criminal sanctions regarding Eurocrimes. As an integral part of this methodological approach, each module concludes with a dedicated section for Key Findings. These concise cores of scientific summary serve as genuine conceptual anchors, structured in an immediate nominal style to recapitulate the fundamental outcomes of each criminal sphere, guiding the reader toward an organic and well-defined overview.

Through this collection, the EU-GLOBACT Module pursues the goal of ensuring the long-term sustainability of its strategic impact by capitalizing on and systematizing the results achieved, thereby securing their continuity and institutional vitality even after the co-funding cycle by the European Commission has concluded. This core ambition will be achieved through the maintenance and constant continuation of dissemination activities for EU-GLOBACT scientific products, including this *Handbook*, which will be officially included and integrated into the required and suggested readings for students of the various courses taught by the Module Leader and the teaching staff. The contributions of this work will thus enrich the curricula of the chairs of *Institutions of International Law*, *European Union Law*, *Diplomatic and Consular Law*, *European and International Criminal Law*, as well as the new Legal Writing Laboratory on *Transnational Crime and Judicial Remedies*, activated as a permanent educational output of EU-GLOBACT within the Department of Legal Sciences starting from the academic year 2026/2027.

*1 August 2026*

# EU Judicial Cooperation in Criminal Matters

*by Anna Oriolo*[*]

SUMMARY: I. Introduction – II. EU (*Indirect*) Competence in Criminal Matters – III. EU Criminal *Direct* Competence, the EPPO, and Financial Protection.

KEY WORDS: EPPO; Eurocrimes; EU Financial Interests; Judicial Cooperation; Transnational Crime.

## I. Introduction

Transnational crimes (or cross-border crimes) are so-called "multinational" criminal phenomena (including offences linked to organised groups, businesses, and political lobbies) that transcend national borders, violate the laws of different States, or have an impact on more than one nation. These offences are emblematic of the link between internal and external security: they represent a significant threat to individuals and communities, businesses, national institutions, and the economy as a whole. Indeed, perpetrators of acts of terrorism and other organised crimes use their massive illegal profits to infiltrate the economy and institutions, including through corruption, thereby eroding the rule of law and fundamental rights, undermining the global security, and damaging their trust in public authorities.

Furthermore, **global emergencies**, such as armed conflicts, health emergencies, and natural disasters, amplify the threat that cross-border offences pose to the values and interests of the global community and to international security security: the **Russia-Ukraine crisis**, the **Covid-19 pandemic**, and **environmental disasters** caused by climate change have created lucrative opportunities for transnational crime.

Commonly, the legal framework for countering transnational crimes is applied through state criminal justice systems, namely by criminalising specific behaviours in national legislation and prosecuting and punishing the offenders within those individual States. This **criminal justice approach** is reflected in the main international instruments for combating serious crimes of a transnational nature, such as **the 2000 United Nations Convention against Transnational Organized Crime (Palermo Convention, UNTOC)**. The UNTOC deliberately does not contain a strict definition of cross-border crimes, nor does it list them, preferring instead to focus on the **transnational "nature" of these violations**. This choice allows for a broader applicability of its provisions to new types of crime that may emerge over time as global, regional, and local conditions evolve.

[*] Associate Professor of International Law, University of Salerno; IECLO Director; EU-GLOBACT Scientific Coordinator; JICL General Editor.

**REFERENCES**

**UNTOC, 2000, Art. 3 para. 2 , Scope of application**

"For the purpose of paragraph 1 of this article, an offence is transnational in nature if:
(a) It is committed in more than one State;
(b) It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
(c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
(d) It is committed in one State but has substantial effects in another State."

## II. EU (*Indirect*) Competence in Criminal Matters

The definition contained in Article 3(2) of the UNTOC covers a whole range of cross-border violations of general interest that require a "global response" through cooperation among States, similarly to "international" crimes or core international crimes (such as war crimes, crimes against humanity, genocide, and crimes against peace), even though the latter do not necessarily (directly) involve multiple countries.
To tackle these constantly evolving challenges, the European Union adopted a new Common Strategy to combat transnational crime in 2021 as part of its EU Security Strategy, ensuring it can act as a united, more influential **"global actor"** and strengthen international cooperation.
For over a decade the EU has been adopting a series of criminal law measures to combat offences of cross-border interest, aiming for a degree of uniformity in definitions and sanctions for certain very serious crimes, such as terrorism, trafficking in human beings and drugs, and fraud affecting the Union's financial interests. Indeed, **Article 29 of the Treaty on European Union** (TEU) already tasked the EU with "providing citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation in criminal matters". However, until the entry into force of the **Treaty of Lisbon in 2009**, an explicit legal basis for EU competence in the field of transnational crime was lacking, meaning that only a very limited number of such measures fell within the scope of Union policies.

**CASE STUDY**

**Court of Justice of the European Union, Commission v. Council, 2005**

Nevertheless, in a landmark 2005 judgment on an environmental matter the EU Court of Justice stated that although, at the time, neither criminal law nor the rules of criminal procedure fell within the competence of the (then) Community, this "cannot, however, prevent the Community legislature, when the application of effective, proportionate and dissuasive criminal penalties by the competent national authorities is an essential measure for combating serious environmental offences, from taking measures which relate to the criminal law of the Member States which it considers necessary in order to ensure that the rules which it lays down on environmental protection are fully effective", as written in para. 49.

Currently, however, Articles 82 and 83 of the Treaty on the Functioning of the European Union (TFEU) expressly recognize, and in much greater detail than the aforementioned Article 29 TEU, the EU's competence in procedural and substantive criminal law to ensure a high level of (common) security through the approximation of national criminal legislations, if necessary. The Treaty of Lisbon also introduced Article 86 TFEU, which

allows the Council, by means of regulations, to establish a European Public Prosecutor's Office (EPPO) to combat serious crimes affecting the financial interests of the Union.
With regard to **"procedural" criminal competence, Article 82 TFEU** mandates the European Parliament and the Council to establish "**minimum rules**" to facilitate the **mutual recognition of judgments** and judicial decisions, as well as **police and judicial cooperation in criminal matters** having a cross-border dimension. In particular, paragraph 2 of Article 82 TFEU allows the Union to establish minimum rules concerning the **rights of individuals involved in criminal proceedings**. These minimum rules have been progressively established by the European legislator through a series of directives concerning specific rights (such as the right to interpretation and translation, the right to information in criminal proceedings, the right of access to a lawyer, the right to be present at the trial, etc.), leaving national authorities of the EU Member States "the choice of form and methods" to achieve the common result. The reliance on directives to regulate this matter has created a "systemic defect", since, despite providing for "common" rules regarding the EU's criminal competence, Member States organize the procedures for transposing and implementing these rules (contained in directives) in different ways.

**REFERENCES**

**TFEU, Art. 82**

"1. Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83.
The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to:
(a) lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions;
(b) prevent and settle conflicts of jurisdiction between Member States;
(c) support the training of the judiciary and judicial staff;
(d) facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions.
2. To the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension, the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules. Such minimum rules shall take into account the differences between the legal traditions and systems of the Member States.
They shall concern:
(a) the mutual admissibility of evidence between Member States;
(b) the rights of individuals in criminal procedure;
(c) the rights of victims of crime;
(d) any other specific aspects of criminal procedure which the Council has identified in advance by a decision; for the adoption of such a decision, the Council shall act unanimously after obtaining the consent of the European Parliament.
Adoption of the minimum rules referred to in this paragraph shall not prevent Member States from maintaining or introducing a higher level of protection for individuals.
3. Where a member of the Council considers that a draft directive as referred to in paragraph 2 would affect fundamental aspects of its criminal justice system, it may request that the draft directive be referred to the European Council. In that case, the ordinary legislative procedure shall be suspended. After discussion, and in case of a consensus, the European Council shall, within four months of this suspension, refer the draft back to the Council, which shall terminate the suspension of the ordinary legislative procedure."

As for **EU "substantive" criminal law**, it can be harmonized through:

- Article 83(1) TFEU, which governs the so-called **Eurocrimes**;
- Article 83(2) TFEU, which concerns the **implementation of EU policies**;
- Article 325(4) TFEU, relating to the **protection of the EU's financial interests**.

Turning to the examination of Article 83 TFEU, pursuant to paragraph 1 of the provision in question, the Union's competences in substantive criminal law concern the adoption of minimum rules on the definition of criminal offences and sanctions in specific "areas of particularly serious crime with a cross-border dimension".
This is an autonomous but indirect criminal competence, exercised through directives, which are acts that, as stated, are not self-executing by nature, binding Member States to certain objectives to be achieved while leaving them free to choose the appropriate means to reach that result. This **indirect competence** specifically covers a list of **Eurocrimes** set out in paragraph 1 of Article 83, namely: **terrorism**, **trafficking in human beings and sexual exploitation of women and children**, **illicit drug trafficking**, **illicit arms trafficking**, **money laundering, corruption**, **counterfeiting of means of payment**, **computer crime**, and **organised crime**. To these, an additional offence was added at the end of 2022 via a specific decision of the Council of the EU, which introduced the **violation of EU restrictive measures**.

**REFERENCES**

**TFEU, Art. 83**

"1. The European Parliament and the Council, acting by means of directives in accordance with the ordinary legislative procedure, may establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.
These areas of crime are the following:
terrorism,
trafficking in human beings and sexual exploitation of women and minors,
illicit drug trafficking,
illicit arms trafficking,
money laundering,
corruption,
counterfeiting of means of payment,
computer crime,
organised crime,
violation of Union restrictive measures.
On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph. It shall act unanimously after obtaining the consent of the European Parliament.
2. If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76.
3. Where a member of the Council considers that a draft directive as referred to in paragraph 1 or 2 would affect fundamental aspects of its criminal justice system, it may request that the draft directive be referred to the European Council. In that case, the ordinary legislative procedure shall be suspended. After discussion, and in case of a consensus, the European Council shall, within four months of this suspension, refer the draft back to the Council, which shall terminate the suspension of the ordinary legislative procedure.
Within the same period, in case of disagreement, and if at least nine Member States wish to establish enhanced cooperation on the basis of the draft directive concerned, they shall inform the European Parliament, the Council and the Commission accordingly. In such a case, the authorisation to proceed with enhanced cooperation referred to in Article 20(2) of the Treaty on European Union and Article 329(1) of this Treaty shall be deemed to be granted and the provisions on enhanced cooperation shall apply."

## III. EU Criminal *Direct* Competence, the EPPO, and Financial Protection

**Article 325(4) TFEU** allows the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, to adopt specific measures in the field of prevention and the **fight against fraud affecting the financial interests of the Union**, an area in which a body of pre-Lisbon legislation already exists.

**REFERENCES**

**TFEU, Art. 325, para. 4**

"The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, after consulting the Court of Auditors, shall adopt the necessary measures in the fields of the prevention of and fight against fraud affecting the financial interests of the Union with a view to affording effective and equivalent protection in the Member States and in all the Union's institutions, bodies, offices and agencies."

Every year, EU Member States detect and report **cross-border fraud** amounting to billions of euros, including a loss of at least **50 billion euros in value-added tax (VAT)**. However, national measures to combat large-scale transnational financial crimes remain limited and are unable to effectively protect the Union's budget. Similarly, neither the European Anti-Fraud Office (**OLAF**), nor the EU judicial cooperation unit (**Eurojust**), nor the European Union Agency for Law Enforcement Cooperation (**Europol**) are empowered to initiate investigations or criminal prosecutions within the Member States.
In response, the Council of the European Union, acting in accordance with Article 86 TFEU, adopted **Regulation (EU) 2017/1939** establishing **the European Public Prosecutor's Office (EPPO)**, which is tasked with investigating and prosecuting the perpetrators of fraud and other offences affecting "**the financial interests of the Union**". These interests encompass the management of budget appropriations, as well as all cases impacting the assets of the EU and those of the Member States, such as fraudulent activities related to Union funds (for instance, the use or presentation of false, incorrect, or incomplete statements or documents resulting in the misappropriation, misapplication, or wrongful retention of funds or assets from the Union budget or budgets managed by the Union or on its behalf), collectively referred to as "**PIF offences**".
Fraud affecting the financial interests of the Union includes "serious" offences against the common EU VAT system, such as those connected to the territory of two or more Member States and involving a total damage of at least ten million euros (namely, the use or presentation of false, incorrect, or incomplete VAT-related statements or documents, or the non-disclosure of VAT-related information in violation of a specific obligation, having the effect of reducing the Union's budget resources). However, the EU's financial interests can also be compromised or threatened by money laundering, corruption, and misappropriation.
Furthermore, the *ratione materiae* competence of the **EPPO extends to ancillary offences** deemed to be "inextricably linked" to PIF offences, such as acts aimed at securing the material or legal means to commit offences affecting the Union's financial interests or to secure the profit or proceeds thereof. Moreover, the European Public Prosecutor's Office can investigate and prosecute offences related to organised crime (including membership, organisation, and leadership of a criminal organisation) when the objective of such an illegal network is to commit PIF offences. Finally, Article 86 (4) TFEU provides that **the European Council** (acting unanimously after obtaining the consent of the European Parliament and after consulting the Commission) **may amend the powers of the EPPO and extend them to cover other serious crimes** that "have a cross-border dimension" and "implications in more than one Member State", such as terrorism and environmental crime.

**REFERENCES**

**TFEU, Art. 86**

"1. In order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust. The Council shall act unanimously after obtaining the consent of the European Parliament.
In the absence of unanimity in the Council, a group of at least nine Member States may request that the draft regulation be referred to the European Council. In that case, the procedure in the Council shall be suspended. After discussion, and in case of a consensus, the European Council shall, within four months of this suspension, refer the draft back to the Council for adoption.
Within the same timeframe, in case of disagreement, and if at least nine Member States wish to establish enhanced cooperation on the basis of the draft regulation concerned, they shall notify the European Parliament, the Council and the Commission accordingly. In such a case, the authorisation to proceed with enhanced cooperation referred to in Article 20(2) of the Treaty on European Union and Article 329(1) of this Treaty shall be deemed to be granted and the provisions on enhanced cooperation shall apply.

2. The European Public Prosecutor's Office shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, offences against the Union's financial interests, as determined by the regulation provided for in paragraph 1. It shall exercise the functions of prosecutor in the competent courts of the Member States in relation to such offences.

3. The regulations referred to in paragraph 1 shall determine the general rules applicable to the European Public Prosecutor's Office, the conditions governing the performance of its functions, the rules of procedure applicable to its activities, as well as those governing the admissibility of evidence, and the rules applicable to the judicial review of procedural measures taken by it in the performance of its functions.
4. The European Council may, at the same time or subsequently, adopt a decision amending paragraph 1 in order to extend the powers of the European Public Prosecutor's Office to include serious crime having a cross-border dimension and amending accordingly paragraph 2 as regards the perpetrators of, and accomplices in, serious crimes affecting more than one Member State. The European Council shall act unanimously after obtaining the consent of the European Parliament and after consulting the Commission."

# International Terrorism

*by Luisanna Savino*[*]



KEY FINDINGS: Dogmatic transition of the phenomenon; Relevance of specific intent in the definition; Anticipation of the punishability threshold (Advanced prevention); Subsidiary role of Artificial Intelligence and administrative limits; Consolidation of the mutual recognition model.

## I. Why does International Terrorism Represent an Asymmetric Threat of Global Interests and What Political Tensions Hinder a Unified Definition?

**International terrorism** is a criminal phenomenon toward which the attention of the international community had already focused on the eve of World War II, and it still remains an element of extreme relevance within the agenda of States and main international organizations.

Traditionally framed within the category of **transnational crimes** – meaning illicit conducts that, despite carrying international significance, do not fall under the jurisdiction of international tribunals, as their repression is handed over exclusively to individual States – international terrorism has assumed a **new legal and political configuration** following the events of **September 11, 2001**: given the tragedy of those events, a progressive recognition of the phenomenon within the framework of **international crimes** has taken place.

Despite the centrality of the phenomenon, the **legal definition** of international terrorism remains controversial. This is due to its intrinsic complexity, historical layering, and multi-faceted nature, elements that make it hard to elaborate a single shared definition at

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

the international level. Indeed, one of the problems that most hinders the fight against terrorism is the **lack of agreement on the definition** of terrorism itself.
The core of this problem lies within the **underlying political tensions**:

- On one side, there is a **broad alignment of countries and scholars** who believe that the definition of international terrorism **should not include** the actions of those who fight for the freedom of their people, oppressed by a foreign occupation, as frequently recalled in the debate surrounding the **Israeli-Palestinian conflict**.
- On the other side stands a **group of States and experts** who point out that what must be considered is **the act itself**, regardless of the context in which it occurs or its underlying motivations: an act, therefore, can be qualified as international terrorism even if framed within the struggle for the assertion of the **principle of self-determination of peoples**.

These divergences within the international community became evident on numerous occasions within the **UN General Assembly**, demonstrating the fear that an excessive exploitation of the notion of terrorism could lead to qualifying as terrorists those figures fighting to obtain the independence of their peoples under the principle of self-determination. In this context, the **Palestinian question** has been frequently cited as an emblematic example of such tensions.
Historical events have demonstrated that international terrorism has always assumed different forms and is, therefore, in **continuous evolution**. During and after World War I, acts of terrorism took on a central role as tools of struggle for the liberation of peoples subjected to foreign occupation, as demonstrated by partisan struggles. Subsequently, international terrorism was understood as a form of **planned and systematic violence**, exercised especially in urban contexts and against State entities by clandestine groups pursuing objectives of a political nature. It has also been highlighted how terrorism is an extremely complex and articulate phenomenon, seeing the **intersection between criminology and politics**, expressing itself through dynamics of war, propaganda, and, in some cases, religion.

**FOCUS**

**A. Schmid, Political Terrorism: A Research Guide, 1983**

Within the international sphere, the definition by Schmid is well-known and considered conventional by many, especially in the United States:
"Terrorism is a method of combat in which random or symbolic victims serve as instrumental targets of violence. The members of a group are placed in a state of chronic fear (terror), derived from previous acts of violence or the credible threat of violence. The victimization of the target group is considered abnormal by most observers [...] which in turn creates an audience of spectators beyond the immediate target of terror [...]. The purpose of terrorism is either to immobilize the target of terror to produce disorientation and/or acquiescence, or to mobilize secondary targets."

In general, international terrorism presents certain **distinctive traits** identifiable in the adoption of **calculated acts of violence** against individuals and groups, aimed at creating a climate of intimidation and terror, and often at causing death in the name of political or religious purposes. It is, however, appropriate to note how the **Security Council**, in **Resolution 1373** adopted in September 2001, affirmed that **it is not necessary to provide a unified definition** for this international crime to elaborate the most effective possible protections against the phenomenon.

The approach of this resolution, which represented a **turning point** in the fight against international terrorism by imposing **binding obligations** on Member States regarding prevention and enforcement, demonstrates that one must not focus on the etymology of the phenomenon, but rather on the **motivations of terrorist groups**, on their **modalities, and strategies**. The Security Council, in fact, preferred not to dwell on the legal definition of "international terrorism", but rather adopted the objective of elaborating **urgent and concrete measures** to strengthen international cooperation.

International law provides a series of protections against terrorism; in particular, it drives States to **cooperate effectively** with one another in preventing and fighting the crime. This discipline is articulated across various legal instruments aimed at regulating specific profiles of enforcement against terrorism, integrated by further international conventions and treaties intended to regulate cooperation in criminal matters, the protection of refugees, as well as the rules relating to the **law of armed conflicts**.

The international regulatory framework must be integrated with what has been laid out by the **European Union (EU)**, which, following the events of September 11, 2001, activated itself especially in the area of **Common Foreign and Security Policy (CFSP)** to identify terrorist groups and entities, implementing measures against the financing of terrorism with acts such as the **freezing of financial assets and economic resources** belonging to the terrorist groups themselves. In a series of regulatory acts adopted in December 2001, the European Council proposed specific tools to fight international terrorism, even establishing a true *black list* for persons and entities involved in terrorist activities.

The EU, therefore, significantly intensified its internal processes of cooperation and integration in the face of terrorist aggression, despite the discordant orientations adopted by individual national governments.

**FOCUS**

**Specialized European Union Agencies against Terrorism**

The institutional integration of the European Union against the terrorist threat consolidated thanks to the establishment and reinforcement of specialized agencies within the Area of Freedom, Security, and Justice:

- **Europol (1998):** Central hub for intelligence exchange and coordination of national police forces, reinforced with the European Counter Terrorism Centre (ECTC).
- **Eurojust (2002):** Organism aimed at implementing judicial cooperation in criminal matters among magistrates of Member States for the prosecution of cross-border terrorist offenses.
- **ENISA (2004):** European Union Agency for Cybersecurity, essential for preventing structured cyber-attacks on critical infrastructures managed by terrorist cells (cyber-terrorism).
- **Frontex (2005):** Agency for the control and security of the external borders of the Union, fundamental for intercepting the flows of foreign terrorist fighters.

## II. What are the Essential Elements Required to Define the Crime of Terrorism?

Despite the considerable doctrinal and political divisions previously highlighted, there are several essential elements that are typically considered regarding the definition of the crime of international terrorism. These prerequisites, derived from numerous international conventions on the matter and declarations of the UN General Assembly, can be summarized into three peculiar characteristics:

- **Intent to spread terror:** The eversive action is programmatically oriented toward instilling chronic fear within the civil population or segments of it.
- **Indiscriminate nature of the attack:** The conducts strike indiscriminately, deliberately overriding the core international law principle of distinction between civilians and combatants.
- **Presence of an eversive specific intent:** The action is guided by precise ideological, political, religious, racial, or ethnic-national purposes.

Furthermore, to fully understand the phenomenon, it is important to consider that these acts constitute a **violation, or a threat, to values of universal relevance** such as international security and peace, likewise harming the protective prerogatives held by diplomatic agents and UN officials.

Under the profile of **multilevel dogmatic qualification**, it should be noted that terrorism, depending on the circumstances in which it occurs, can be linked to the categories of *crimina iuris gentium*:

- **War crime:** Where the conduct is inserted and perpetrated within the context of an armed conflict, whether international or internal.
- **Crime against humanity:** In the hypothesis where the terrorist act is part of a widespread, massive, and systematic attack directed against the civilian population.

Ultimately, international terrorism **does not currently fall** under the material competence of the Rome Statute of international criminal courts. However, in light of the severe events of recent years and the emergence of a global form of terrorism, States could evaluate the opportunity of this choice and decide to attribute competence over terrorism to the **International Criminal Court (ICC)** or create an *ad hoc* special tribunal for these crimes.

The attacks of **September 11, 2001**, in New York and at the Pentagon marked the establishment of a **new generation of terrorist activities**, which raised growing concerns within the international community. The fact that the United States suffered the most significant terrorist attack ever organized highlighted above all the **transnational organizational framework** possessed by certain terrorist groups such as, for instance, *Al-Qaeda*, which distinguished itself by its complete **financial autonomy** from States, acting as a global asymmetric actor.

This triggered, in particular, the fear throughout the West that Osama Bin Laden's terrorist network might attempt to acquire **weapons of mass destruction (WMD)**. These concerns emerged as early as October 2001. In this context, the **International Convention for the Suppression of Acts of Nuclear Terrorism of April 13, 2005**, assumes particular importance, aimed at establishing a common legal basis to prevent, prosecute, and punish acts of terrorism involving nuclear materials and devices. In particular, the Convention specifies the criminal figure of **nuclear terrorism**.

**REFERENCES**

**International Convention for the Suppression of Acts of Nuclear Terrorism, 2005, Art. 2**

"Any person commits an offense within the meaning of this Convention if that person unlawfully and intentionally: (...) Makes use in any way of radioactive material or a device, or uses or damages a nuclear facility in such a manner as to cause or risk causing the release of radioactive material: (i) with the intent to cause death or serious bodily injury; or (ii) with the intent to cause substantial damage to property or to the environment; or (iii) with the intent to compel a natural or legal person, an international organization or a State to do or refrain from doing any act."

Further structural changes occurred after September 11: international terrorism began to **exploit modern technologies** to establish itself and instil fear. Specifically, with the war in Iraq in 2003, a specific strategy of terrorist groups emerged, aimed at **maximizing the media dissemination** of every single attack. This technique proved particularly effective in the kidnappings of Western journalists and workers, followed by the broadcasting of images and news across media platforms, **amplifying the global psychological impact** of the events.

To best understand the post-9/11 phenomenon of international terrorism, it is fundamental to consider the proposal for a Council of the European Union framework decision on the fight against terrorism, presented by the Commission in September 2001, which laid the groundwork for criminal harmonization within the European area.

**REFERENCES**

**Proposal for a Council Framework Decision on Combating Terrorism (COM/2001/521 Final, Explanatory Memorandum), 2001**

"Terrorism is an old phenomenon but, unlike in the past, today's terrorism is particularly dangerous as the real or potential impact of armed attacks is increasingly devastating and lethal. This is due to the growing sophistication and fierce ambition of terrorists, as recently demonstrated by the tragic events of September 11 in the United States, or to technological developments, both regarding traditional weapons and explosives and regarding even more terrifying tools such as chemical, biological, and nuclear weapons. Furthermore, new forms of terrorism are emerging. The profound changes in the nature of terrorist offenses show the inadequacy of traditional forms of judicial and police cooperation in the fight against terrorism. […] Given the absence of borders within the European Union and the fact that the right to free movement of persons is guaranteed, it is necessary to take new measures regarding the fight against terrorism. Terrorists can take advantage of the differences in legal treatment across different Member States."

Understanding the current threat landscape requires a preliminary overview of global terrorism, with a specific focus on **the evolution of characteristics of terrorist groups**:

- **First Generation (Traditional-National Phase):** Rigid and pyramidal hierarchical structures, strong dependence on the logistical or financial support of specific state sponsors, actions targeted at local or regional levels for self-determination.
- **Second Generation (Al-Qaeda Phase - Post-9/11):** Transnational network with a molecular character, total financial autonomy from States, digitalization of propaganda, and systematic exploitation of global media resonance.
- **Third Generation (Contemporary Scenario)**: Fluid reticular structures (hub-and-spoke), lone wolves radicalized on the web, use of decentralized technologies (cryptocurrencies, darknet channels), and the constant threat of cyber-terrorism.

Recently, the terrorist association that has raised the most concerns across the international community overall is the Islamic State (**ISIS** or *Daesh*). This entity distinguishes itself from all previous terrorist groups, particularly from *Al-Qaeda*, due to the nature of its communicative strategy: **ISIS features a utopian-type propaganda** centred on the immediate construction and territorial governance of a self-proclaimed global caliphate, unlike *Al-Qaeda* which always maintained a predominantly **nihilistic** propaganda direction of pure asymmetric destruction of the Western adversary. Thus, the contemporary terrorist threat constitutes an unprecedented challenge to peace among nations, the stability of international relations, and the internal security of States across all geopolitical areas.

## III. How do the UN and NATO Shape the Global Counter-Terrorism Response?

The **United Nations (UN)** was born with the signing of the Charter of the United Nations on June 26, 1945, in San Francisco. Composed of 193 members, representing almost the entirety of the international community, it is the highest multilateral organization aimed at promoting international peace and security. Within the Charter, there are already regulatory elements indicating the organization's purposes, specifically in Art. 1 and Art. 2. Furthermore, Art. 103 of the Charter establishes a *supremacy clause* asserting the preeminence of the UN over "other" obligations incumbent upon Member States in the event of a conflict between such obligations and the UN Charter, or the obligations arising therefrom.

**REFERENCES**

**Charter of the United Nations, 1945, Art. 103**
In the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail. This provision constitutes the supremacy clause (*supremacy clause*) asserting the **preeminence of the UN Statute** and the binding decisions of its organs over any other treaty obligations binding Member States.

In line with its objectives, the **UN Global Strategy** against international terrorism consists of adopting measures structured around **four essential purposes**:

- **Countering the conditions** conducive to the spread of the phenomenon (e.g., conflict resolution, socio-economic development).
- **Preventing and combating** terrorism as such, by depriving groups of operational and financial resources.
- **Developing the capacity of States** to face the threat, strengthening bilateral technical assistance.
- **Ensuring respect for human rights** and the rule of law as the fundamental basis for the fight against terror.

In this framework, the **General Assembly**, the only organ in which all Member States hold the right to vote, plays a fundamental role in elaborating a legal framework to promote international cooperation. The Assembly operates through subsidiary organs termed **Standing Committees**, composed of representatives from all States. Among these, the following play a crucial role in countering eversion:

- **The Third Committee (Social, Humanitarian and Cultural Committee):** Deals with issues relating to human rights and their preventive protection, monitoring that emergency enforcement laws do not violate fundamental freedoms.
- **The Sixth Committee (Legal Committee):** A technical-legal organ which in 1994 adopted the Declaration on Measures to Eliminate International Terrorism.

Furthermore, the General Assembly established, via Resolution 51/210 of 1996, an ad hoc Committee (Ad Hoc Committee) which led to the adoption of the International Convention for the Suppression of the Financing of Terrorism (New York, 1999) and the International Convention for the Suppression of Acts of Nuclear Terrorism (2005). Since 2001, this Committee has held the mandate to draft a **Comprehensive Convention on International Terrorism** aimed at elaborating a general, abstract, and unified definition of terrorist offenses, applicable also to hypotheses not governed by older sectoral conventions. To date, however, due to well-known political divisions over the notion of a terrorist, this Convention **has not yet entered into force**. In 2006, the Assembly consolidated this path by officially adopting Resolution 60/288, which established the **United Nations Global Counter-Terrorism Strategy**.

Regarding the **Security Council**, it plays a central role in operational enforcement against the phenomenon. Composed of fifteen members, including **five permanent members with veto power** (China, France, Russian Federation, United Kingdom, and United States), it intervenes through binding resolutions under Chapter VII of the UN Charter and targeted sanctions regimes (*targeted sanctions*). One of the most relevant instruments in the history of international law is **Resolution 1373** adopted on September 28, 2001, in the immediate aftermath of the September 11 attacks. With this act, the Council qualified terrorist attacks as a threat to international peace and security, reaffirming the **right to individual and collective self-defence** under Art. 51 of the UN Charter.

**REFERENCES**

**UN Security Council, Resolution No. 1373, 2001, Operative Paragraph 2**

"Decides that all States shall: (a) Refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists; (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information; (c) Deny safe haven to those who finance, plan, support or commit terrorist acts, or provide safe havens; (d) Prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens."

The centrality of Resolution 1373 lies finally in its establishment, under operative Paragraph 6, of the **Counter-Terrorism Committee (CTC)**, tasked with monitoring the implementation of obligations by all members.

The ratio behind establishing the Counter-Terrorism Committee (CTC) is to create a permanent and superior forum to which all Member States have the legal obligation to periodically provide reports and information regarding the status of adjustment of their domestic criminal laws. The organ considers terrorism a serious violation of international peace and security, thus justifying the adoption of counter-measures in all its forms, in accordance with the principles established by the UN Charter. This monitoring and verification activity on the field was subsequently strengthened and institutionalized by the Security Council through Resolution 1535 of 2004, which established the Counter-

Terrorism Committee Executive Directorate (CTED), a special executive office designed to provide direct technical and operational support to the Committee itself.
Ultimately, it can be noted that the traditional approach to the terrorist phenomenon, based on mere domestic prevention and criminal repression, is today inadequate in light of the exceptional development and growing transnational complexity reached by terrorist organizations. These have structured criminal networks capable of jeopardizing one of the most essential international public goods: security, launching a direct attack against the democratic, civil, and political values of the global community. The cross-border width of the phenomenon has generated no small difficulties in the elaboration of a general international convention on the matter by the UN, leaving room for the intervention of European regional legislators.
In addition, the role played by **NATO** is also central in the analysis of counter-strategies, especially following the terrorist attacks of September 11, 2001. In this context, the Alliance recognized terrorism as a **threat to collective security** and progressively developed various measures to face it. The reaction of NATO to the attacks against the United States was immediate and of particular legal relevance: for the first time, in fact, Member States decided to **activate Art. 5 of the Washington Treaty**, namely the **collective defense clause** (also recognized by Art. 51 of the UN Charter). In doing so, NATO formally brought the legal effects of asymmetric terrorist acts under the traditional notion of an **armed attack**.
NATO's commitment materialized through a growing cooperation with partners and international organizations, particularly with the United Nations. Relevant under this profile was the role played by the Alliance in **Afghanistan**, which contributed to structuring global counter-terrorism cooperation on the field. The Atlantic Alliance, thanks to its **transatlantic dimension**, its dense network of global partnerships, and its own operational capacities of *intelligence-led defence*, is therefore capable of bringing a lasting contribution to the continuous challenge against international terrorism.

**FOCUS**

**The NATO-ICI Strategic Framework in Combating Terrorism**

- Activation of Art. 5 NATO Treaty (Post-9/11): Equating the effects of an asymmetric terrorist attack to a traditional armed attack, activating the right to collective self-defense under Art. 51 of the UN Charter.
- Positive Obligations *ex* ICSFT Convention (1999): Duty of States to criminalize financing, freeze suspicious funds, cooperate in criminal assistance, and apply the rule of *aut dedere aut judicare*.
- Scope of the ICJ Judgment of January 31, 2024: Delimitation of the scope of application of the ICSFT Convention. It hits individual crimes of financing (even if committed by state organs) but does not configure a direct responsibility of the State for eversive acts of its own emanation, while imposing the strict duty to investigate suspects (Art. 9 ICSFT).

A crucial aspect to consider in this context is the issue of the state liability in the financing of terrorism. The **International Convention for the Suppression of the Financing of Terrorism (ICSFT)** is a United Nations treaty adopted by the General Assembly in 1999 through Resolution 54/109. Its main purpose is to prevent, suppress, and punish the financing of terrorist acts, preventing financial flows, funds, and assets from being used to support such activities. The Convention specifically defines the concept of terrorism financing, including all operations aimed at providing, collecting, or employing resources for the realization of eversive acts, and establishes **precise positive obligations of**

**criminalization and cooperation** binding Member States. It represents, therefore, a fundamental multilevel tool to hit terrorist groups in their vital financial resources.
In relation to the application of the ICSFT and the International Convention on the Elimination of All Forms of Racial Discrimination (CERD), the **international litigation between Ukraine and the Russian Federation** carries a cornerstone academic significance. Ukraine's appeal originates from the geopolitical events occurring from 2014 onward in the eastern area of the Country (Donbass) and in Crimea. Kyiv lamented the violation, by Moscow, of the obligations provided by the Convention, accusing it of having provided funds, heavy weapons, and operational support to illegal armed groups (such as the militias of the Donetsk and Luhansk People's Republics) responsible for severe attacks against civilians, including the **downing of Malaysia Airlines Flight MH17**.
Ukraine claimed direct **State responsibility** of the Russian Federation for having, through its state organs and other agents, subsidized the preparation and commission of terrorist acts perpetrated by non-state actors. The case concluded on **January 31, 2024, with the judgment on the merits by the International Court of Justice (ICJ)**.

**CASE STUDY**

**International Court of Justice, Ukraine v. Russian Federation Judgment, 2024**

The ruling of January 31, 2024, represents the **first judgment on the merits by the International Court of Justice on the ICSFT Convention** and offers crucial points of reflection for legal doctrine, given the scarcity of judicial precedents on international terrorism. The ICJ issued a very strict decision under a literal profile, clarifying that **the ICSFT Convention does not directly govern the financing of terrorism by the State as such (State-sponsored terrorism)**, but forbids and represses financial conduct when it is perpetrated by **individual physical persons** (be they private subjects or single state organs acting individually). Therefore, the Convention imposes positive obligations of prevention and repression of illicit conduct on one's own territory, regardless of the nature of the authoring subject.
In the specifics of the judgment, the Court was called upon to verify the violation of various conventional obligations:

- **Art. 8**, on measures of identification, freezing, or seizure of illicit funds.
- **Art. 9, para. 1**, relating to the **obligation to investigate** and look into reports of suspected subjects on one's territory.
- **Art. 10**, which enshrines the cornerstone principle of international criminal law ***aut dedere aut judicare*** (extradite or prosecute).
- **Art. 12, para. 1**, in matters of assistance and mutual cooperation in criminal investigations.
- **Art. 18, para. 1**, on the general duty of preventive cooperation and information exchange.

The International Court of Justice excluded the existence of the violations complained of by Ukraine for almost all the cited articles due to a lack of evidence on the specific terrorist intent of the transferred funds (deemed aimed at financing warlike guerrilla warfare but not terrorist acts against civilians under the ICSFT standard). However, the ICJ ascertained the actual violation of Art. 9, para. 1, by Russia, condemning Moscow for the failure to carry out adequate, timely, and genuine investigations regarding the official and detailed reports sent by Kyiv about suspected financiers of terrorism present on Russian territory.

## IV. How do the United Nations Balance Counter-Terrorism Operations with Human Rights?

The protection of human rights in the fight against terrorism proves to be a delicate and complex topic on which, especially in the last decade, the attention of international doctrine and practice has cantered. No unanimous orientation is found, however, regarding which value should prevail when a conflict arises between security requirements and the protection of individuals.
Legal doctrine is historically split around **three macro-ideological approaches**:

- **Criminal Emergency Approach:** Moves from the conviction that the protection of human rights can be legitimately compressed and derogated in function of temporary necessities tied to the security of the State.
- **Case-by-Case Balancing Approach:** Considers that the right of individuals to protection against terrorist violence falls itself among fundamental rights; it follows that States should balance proportional measures between collective security and individual protection.
- **Absolutist Protection Approach:** Considers violations of human rights radically unjustifiable, even if motivated by the eversive purpose of combating the terrorist phenomenon; according to this perspective, States and supranational organizations should always act in line with fundamental guarantees, regardless of security contingencies.

This uncertainty directly involved the UN, which treated the topic especially within the framework of the Third and Sixth Committees of the General Assembly. In particular, the **Third Committee** placed the accent on fundamental profiles such as: the **principle of legality** in the criminalization of acts, the **principle of non-discrimination**, **procedural guarantees**, the **prohibition of torture**, and the obligation of ***non-refoulement*** (prohibition of return toward countries at risk).
Regarding the Sixth Committee, Special Rapporteur Martin Scheinin highlighted how the absence of an agreement on the definition of the phenomenon still blocks the completion of negotiations on the global counter-terrorism Convention.
Among the innovations introduced by the General Assembly, particular attention must be reserved for the **UN Global Counter-Terrorism Strategy (2006)** and the *Counter-Terrorism Implementation Task Force*. The Strategy is of particular relevance since it represents the first comprehensive framework approved at the international level to face the problem. One of its four pillars concerns precisely **respect for human rights and the rule of law** as basic elements; however, Special Rapporteurs highlight how this centrality does not always find matching verification in concrete operational practice of the United Nations.

**FOCUS**

**Operational Criticalities on the Field**

In a particular way, **four core areas** have been identified in which, during counter-terrorism operations on a global scale, possible violations of international norms have been recorded:
1.The modalities of **prolonged detention** and special prison regimes lacking immediate legal assistance.
2.The compression of guarantees of a **fair trial**, due to the use of secret evidence or intelligence sources non-disclosable to the defence.
3.The violation of the **absolute prohibition of torture** and inhuman or degrading treatment during interrogations conducted in conflict zones or offshore detention centres
4.The disproportionate limitation of **other fundamental rights**, such as the freedom of expression, freedom of association, and the right to privacy through mass electronic surveillances.
It has been highlighted by international doctrine how such violations result sometimes perpetrated directly by intergovernmental organizations or multilateral agencies operating on the field. However, the **international legal responsibility of the UN** and of Member States has been frequently excluded or limited by domestic and foreign judicial organs applying the rules on institutional immunities of the United Nations. It emerges, therefore, that despite the General Assembly having paid formal attention to the protection of human rights, in specific operational contexts profound structural criticalities exist that pose the urgent problem of the Organization's responsibility for conducts non-compliant with international obligations.

**FOCUS**

**Limits to Balancing Human Rights in Counter-Terrorism**

- **Absolute Inalienable Rights (Core Rights):** Rights that can never be compressed, not even in situations of military or eversive emergency. They include the right to life, the prohibition of torture, the prohibition of slavery, and the principle of criminal legality penale (*nullum crimen sine lege*).
- **Proportional Derogable Rights:** Rights that admit temporary and proportionate limitations for national security needs, provided they are provided by law and necessary in a democratic society. They include the right to privacy, freedom of movement, freedom of assembly, and freedom of expression.

## V. How has the European Union's Response to the Phenomenon of International Terrorism been Structured?

The fight against terrorism represents by now one of the priority themes for the international community. In particular, the **European Union (EU)**, in its capacity as an international organization and security community, plays a crucial role in preventing and regulating terrorism offenses. Due to its complex nature, the EU has had to face intricate interactions between transnational and governmental levels in elaborating counter-terrorism policies and strategies.
It must be reiterated how, prior to the attacks of September 11, 2001, counter-terrorism measures at the community level were overall **limited and fragmentary**, almost entirely relegated to spontaneous intergovernmental cooperation. The decisive impulse within the **Common Foreign and Security Policy (CFSP)** configures itself, therefore, as a reaction to those tragic events, from which arose a security emergency that led to a progressive, albeit sometimes uneven, regulatory development.

The European Union pursues the objective of **harmonizing national legislations** of individual Member States and has distinguished itself for the constant search for common defense and prevention strategies against the terrorist phenomenon, in coherence with the mutation of the same tied also to new geopolitical assets and the use of new computer technologies.
In this regard, it is important to consider **Common Position 2001/930/CFSP**, a decision of historical significance adopted by the Council of the European Union on December 27, 2001, with the aim of outlining the general principles of the fight against terrorism. This act established a strict legal and operational framework, introducing specific measures:

- The **suppression of any form of support**, active or passive, for entities or persons involved in terrorist acts.
- The adoption of measures to **prevent recruitment** of members by terrorist groups.
- The **elimination of the supply of weapons**, as well as of falsified or fraudulent identity and travel documents.

The main purpose of Common Position 2001/930/CFSP was to give immediate and effective execution within the European legal order to the resolutions of the United Nations Security Council, in particular to **Resolution 1373 (2001)**, binding Member States to apply targeted sanctions and to establish the first official lists (*black lists*) for the freezing of assets.
In addition, given that terrorist organizations for the realization of their illicit activities require huge sums of money and, in general, considerable economic resources (such as armaments, equipment, logistical transfer of human resources, recruitment, and training), the European Union began to impose itself through regulatory acts of judicial cooperation in criminal matters. The first true pillar was **Framework Decision 2002/475/JHA** of June 13, 2002, issued in order to combat international terrorism. This decision indicated as an **activity of participation in a terrorist group** also the conduct of those who provide material or financial resources with full awareness of the eversive purpose of such contribution.
This initiative – subject to subsequent modifications and finally entirely replaced by **Directive (UE) 2017/541** – constitutes the broadest European action of prevention and enforcement against the terrorist phenomenon since, following the latter, a series of coordinated and incisive measures have been arranged, such as the freezing of capital, the blocking of suspicious financial activities, and direct cooperation of judicial police.
The **legal basis** for such a powerful European regulatory production is constituted today by **Art. 82 and 83 of the Treaty on the Functioning of the European Union (TFEU)**. In particular, Art. 83 authorizes the European Parliament and the Council to establish minimum rules aimed at uniforming, among Member States, the definition of offenses and the scale of penalties to apply in relation to criminal phenomena of particular gravity and with a marked transnational dimension.

## VI. How does the European Union Regulate Terrorist Offenses and Related Conduct?

From the outlined regulatory framework, it emerges that over time, and following numerous attacks perpetrated by organizations belonging to the so-called Islamic State (**ISIS**), the European Union has placed the fight against terrorism as an absolute priority.

Despite the progress made, the need to adapt existing legislation to the new face of the threat became clear. In particular, with the aim of intensifying enforcement actions, provisions were introduced to punish behaviours connected to the phenomenon of **Foreign Fighters** – combatants who travel abroad to join terrorist activities, training, or combat.

The attacks perpetrated in Paris and Copenhagen in early **2015** represent some of the most serious episodes of terrorism in recent European history; these events shook world public opinion, prompting European institutions to rapidly evolve the legislative framework to fill the gaps that emerged in preventing and monitoring the flows of radicalized combatants.

The events in the Danish capital on February 14 and 15 that year perfectly illustrate this turning point. The perpetrator, a man of Danish origin inspired by radical Islamist ideologies, was identified as Omar El-Hussein. Both attacks targeted symbolic venues: the first was carried out on February 14 at the Krudttønden cultural center, where a debate on freedom of expression was taking place with the French ambassador to Denmark. El-Hussein opened fire, killing one person and wounding three police officers. The second attack took place in the early hours of February 15 in front of the Great Synagogue in Krystalgade, where a young member of the Jewish community was killed and two other officers were wounded. The perpetrator was eventually killed during a shootout with the police. Both attacks marked a shift in the perception of the terrorist threat in Europe, strengthening international cooperation and raising concerns about the domestic radicalization of young people in Europe.

The EU, therefore, found itself facing a period of high terrorist risk. Despite the political declarations and agendas adopted (such as the European Agenda on Security and the Security Union), the measures implemented – including terrorism alerts, the temporary reintroduction of controls in certain areas of the internal Schengen borders, and an enhanced exchange of information – did not prevent other serious attacks from occurring between 2016 and 2017 in cities such as Brussels, Nice, Berlin, Stockholm, Manchester, and London.

The emergence of new actors, such as ISIS/Da'esh, lone wolves, and *Foreign Fighters*, as well as the evolution of terrorist operational methods, prompted the European Union to review and update its legislation. In March 2017, after months of debate among Member States, the Council and the European Parliament approved **Directive (UE) 2017/541**, repealing the previous Framework Decision 2002/475/JHA. This new act transposed and updated European legislation in light of the growing threat, broadening the concept of terrorist offense and introducing the category of **"related offenses"**. Specifically, in Art. 3 of Title II, terrorist offenses and behaviours attributable to a terrorist group are analytically listed, now including traveling for terrorist purposes and online self-training.

**REFERENCES**

**Directive (EU) 541, 2017, Title II, Art. 3 (Terrorist Offenses)**

Directive (UE) 2017/541 defines, in Art. 3, terrorist offenses as intentional acts which, given their nature or context, may seriously damage a country or an international organization. These acts include: attacks on a person's life, attacks on physical integrity, kidnapping or hostage-taking, and massive destructions (infrastructures, public places), when committed for terrorist purposes.

## VII. What does the Council of Europe Provide Regarding the Prevention of International Terrorism?

As previously highlighted, terrorism represents a growing threat to world security, and the frequency of attacks on European soil has triggered a widespread fear among the population.

The fight against terrorism has become, over time, an absolute priority for the **Council of Europe**, which, since its inception, has reserved a primary role for the **defence of democracy and human rights**. Its organs are called upon to establish effective legal and technical instruments to ensure adequate protection for the population and a rigorous surveillance system. The actions of this institution are based on **three fundamental pillars**:

- **Strengthening the international legal framework:** Through the drafting of binding multilateral conventions that fill the regulatory gaps among Member States.
- **Addressing the causes of terrorism:** Intervening on factors of social vulnerability, intolerance, and isolation that fuel extremism.
- **Protecting fundamental values:** Guaranteeing that criminal enforcement never sacrifices the rule of law, democracy, and individual liberties.

In particular, after September 11, 2001, the firm stance of the Council of Europe has been to seek a **just balance between freedom and security**. A prominent problem in the geopolitical framework is represented by the increase in European citizens who chose to join the ranks of the Islamic State (**ISIS**) in Iraq and Syria. The UN estimated the presence of approximately **25,000 foreign combatants** coming also from European countries (specifically France, the United Kingdom, and Russia).

To face this phenomenon, and in implementation of **UN Resolution 2178 (2014)**, the Council of Europe strengthened its regulatory apparatus through an **Additional Protocol** to the Convention on the Prevention of Terrorism, opened for signature in **2015**. According to the institution, the pursuit of security must never debase the values of democracy; on the contrary, it is necessary to increase protections that are strictly compliant with the **principle of legality** and humanitarian law. This also serves to avoid playing into the ultimate purpose of terrorism, which is to provoke violent, liberticidal, and disproportionate reactions from States.

Regarding the regulatory architecture, the Council of Europe has addressed the problem since the 1970s but intensified legislative production after 2001. The **"Council of Europe Convention on the Prevention of Terrorism"** of May 16, 2005 (Warsaw Convention) assumes a milestone importance. This act focuses on **prevention in the broadest sense**, aiming to fill the gaps in international law identified by **CODEXTER** (Committee of Experts on Terrorism, established in 2003), such as the completion of agreements on extradition and judicial cooperation. Likewise, the Convention qualifies as autonomous criminal offenses those **preparatory instrumental acts** that contribute to the commission of terrorist offenses, including **recruitment**, **training**, and **public provocation**.

**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, Art. 5, Art. 6, and Art. 7**

The Convention imposes on signatory States the obligation to criminalize three key behaviours prior to the terrorist act: public provocation to commit a terrorist offense (Art. 5), recruitment for terrorism (Art. 6), and training for terrorism (Art. 7), understood as providing practical instructions on weapons or explosives with awareness of the eversive purpose.

Building upon this regulatory foundation, the criminalization of preparatory acts is structured around **the three operational pillars of the Council of Europe (Warsaw Convention)**:

- **Public Provocation (Art. 5):** Punishes the distribution of messages to the public that cause a risk of terrorist acts, balancing the sanction with Art. 10 ECHR on freedom of expression.
- **Recruitment (Art. 6):** Incriminates the act of soliciting or inducing another person to commit or participate in a terrorist or associative action.
- **Training (Art. 7):** Configures as an autonomous offense the act of imparting technical instructions for the manufacturing or use of explosives and dangerous substances for eversive purposes.

## VIII. What Role does Artificial Intelligence Perform in European Counter-Radicalization Strategies?

Within the framework of enforcement measures against international jihadist terrorism, the phenomenon of **radicalization** constitutes one of the most complex profiles to intercept. Radicalization refers to all those activities aimed at recruiting new followers and indoctrinating them according to the dictates of extremist ideologies. This concept is highly articulated: part of the doctrine defines it as the psychological and behavioural process through which individuals adhere to violent extremism.

The United Nations delineates **violent extremism** as the beliefs and actions of people who support or employ violence to achieve ideological, religious, or political goals, including terrorism and other forms of structured and politically motivated violence.

Indoctrination often occurs through explicit incitements to embrace slaughterous ideologies, sometimes accompanied by detailed operational instructions for the jihadist cause (such as digital manuals for the artisanal manufacturing of explosive devices or toxic substances). Nowadays, radicalization occurs **prevalently through computer tools**. Although the *dark web* offers greater cryptographic protection from police wiretaps, a massive use of the *surface web* and commercial social networks remains to spread propaganda to an undifferentiated audience. A third form of radicalization is identified in the *online* humiliation of victims of attacks: this conduct, besides offending human dignity, exponentially increases the risk of emotional proselytism among vulnerable subjects.

Therefore, the role of technology is essential in the responses of Western legal systems, both from a regulatory and jurisprudential standpoint. Faced with the pervasiveness of digital propaganda, the need arises to timely curb the phenomenon through **automated tools (intelligent algorithms)** capable of detecting the intrinsic risk of contents and

flagging them for immediate removal, in line with Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online.
This is often followed by the use of criminal law tools to punish the "radicalizer". However, the criminal law approach is not the only applicable path. **Administrative measures of advanced prevention** can be adopted, particularly within the framework of **immigration law**, especially when criminal action proves difficult due to the vagueness or ambiguity of the disseminated messages. If the author of the eversive conduct is a foreigner, domestic authorities can resort to **ministerial expulsion for reasons of national security**.
The main modalities of multilevel administrative intervention include:

- The **preventive denial of entry** or renewal of the residence permit due to a threat to State security.
- The **refusal of assisted repatriation** of one's own citizens (*foreign terrorist fighters* or their family members) detained in foreign conflict zones, if considered subjects with a very high rate of radicalization.

**CASE STUDY**

**European Court of Human Rights, Judgment H.F. v. France, 2022**
An indispensable jurisprudential reference point is the famous ruling of the Grand Chamber in the case *H.F. and Others v. France*. The European Court of Human Rights was called upon to verify whether the refusal by the authorities in Paris to repatriate French women and children (family members of ISIS *foreign fighters*) held in the Syrian prison camps of Al-Hol constituted a violation of Art. 3, para. 2, of Protocol No. 4 to the ECHR (the right to enter the territory of the State of which one is a citizen). The Grand Chamber established that **there is no absolute and automatic right to the repatriation of one's citizens from abroad**, since the State does not exercise effective territorial jurisdiction in those areas. However, the Strasbourg judges imposed on the State the obligation to guarantee a review procedure for repatriation requests that is immune from arbitrariness and equipped with adequate procedural guarantees of judicial review, balancing internal security with the best interests of the minors involved.

In order to intercept these communication flows before they lead to eversive action on the field, modern internet hosting providers (hosting service providers) leverage Artificial Intelligence by applying four main technological tools:

- **Natural Language Processing (NLP):** Analyses textual language to detect suspect content. Through lexical or vector-based analyses, the algorithm evaluates the risk level of the text by analysing critical terms or the recurrence of multiple "tokens" semantically linked to jihadist rhetoric, automatically interpreting the overall communicative context.
- **Image Matching:** Instantly compares images and videos uploaded by users with centralized databases containing extremist material or already known terrorist logos, blocking their upload in real time through *hashing* techniques.
- **Clustering:** Grouping algorithm aimed at cataloguing similar content to identify hidden *patterns*, automated dissemination networks, and connections between profiles that are apparently distant on the web.
- **Recidivism Tackling Algorithms:** Aim to identify radical subjects who continue to create new fictitious accounts to spread eversive content even after the removal of previous ones, using advanced behavioural analysis techniques and device fingerprint tracking.

Technology based on Artificial Intelligence is therefore a key and complementary element in the fight against transnational radicalization: thanks to complex machine learning algorithms, the processes of identification, classification, and assessment of eversive risk have become immediate, proactive, and extremely effective for the security of the European Space.

**REFERENCES**

**Regulation (EU) 784, 2021**
This text imposes on hosting service providers the legal obligation to **remove flagged terrorist content within one hour** from the receipt of the removal order issued by the competent authority of a Member State. The regulation introduces severe sanctions for non-compliant providers and establishes a common framework for the use of automated proactive measures based on Artificial Intelligence.

## IX. How has Domestic Legislation Reacted to and Regulated International Terrorism?

To understand Italian legislation regarding the prevention and contrast of international terrorism, it is first essential to consider **Art. 270 of the Criminal Code**, which, in its original 1930 version, was mainly oriented toward the repression of specific criminal offenses connected to the subversion of the constitutional and political order, predominantly of an **internal nature**.
Following the global impact of terrorism at the international and European level post-September 11, the gaps in the Italian system were filled through **Decree-Law No. 374 of October 18, 2001** (converted with modifications into **Law No. 438 of December 15, 2001**). This landmark reform radically rewrote and amended **Art. 270-*bis* of the Criminal Code**, typifying new associative forms and extending criminal sanctions to the conduct of anyone who promotes, constitutes, organizes, directs, or participates in **associations aiming at the commission of acts of violence for purposes of terrorism, including international terrorism**.

**REFERENCES**

**Italian Criminal Code, Art. 270-*bis* (Associations for the Purpose of Terrorism, Including International Terrorism)**
"Whoever promotes, constitutes, organizes, directs or participates in associations which propose the commission of acts of violence for purposes of terrorism or subversion of the democratic order shall be punished with imprisonment from seven to fifteen years. (...) The purpose of terrorism occurs also when the acts of violence are directed against a foreign State, an eversive institution, or an international organization."

The choices made in 2001 were subsequently expanded, since enforcement actions could not remain merely emergency-based and confined to the traditional associative model alone. The Italian legislator, driven by Euro-unitarian sources, felt the need to abandon an exclusively sector-specific and *ex-post* repressive perspective: there was an urgent need for an **anticipated vision of advanced prevention**, capable of impacting individual behaviours, logistics, and the early identification of those responsible.
Following these objectives, the Italian legal system structured a **double criminal and penitentiary track**, which includes:

- The introduction of **abstract danger offenses with individual conduct**, aimed at punishing preparatory acts prior to the association (such as recruitment *ex* Art. 270-*quater* c.c., training *ex* Art. 270-*quinquies* c.c., and the subsequent incrimination of behaviours connected to *foreign terrorist fighters* and *online* self-training via Decree-Law 7/2015).
- The extension of the **suspension regime of ordinary penitentiary treatment rules *ex* Art. 41-*bis* of the Penitentiary Law** (known as *carcere duro* or harsh prison regime) to subjects detained or convicted for crimes of international terrorism and subversion, in order to sever communication links between the detainee and the external organization.

However, those criminal phenomena which, although qualified as terrorism within individual historical systems, **do not assume a transnational significance**, remain strictly excluded from the notion of international terrorism. This is the case, for example, of the **Red Brigades** (*Brigate Rosse*) in Italy, whose eversive action, although terrorist, structurally exhausted its logistical and political effects within the national territory, without harming interests shared by a plurality of States, without involving foreign cells, and without targeting international organizations.

**CASE STUDY**

**Italian Cassation Court, Fifth Section, Judgment No. 15444, 2023**

In this important ruling, the Supreme Court ruled on the offense of **self-training for activities with purposes of terrorism (Art. 270-*quinquies* c.c.)**, examining the case of a young man who radicalized independently on the *surface web* by downloading ISIS military manuals for manufacturing explosive devices and chemical toxins. The judges of legitimacy established a key principle: for the punishability of individual self-training conduct, interaction with a physical instructor or formal insertion into a cell is not required, but it is indispensable to prove the **suitability and unequivocal nature of the acts** committed by the agent, ensuring that the acquisition of technical instructions is animated by the specific intent (*dolo specifico*) of wanting to commit a subsequent act of terrorist violence, thus excluding from the criminal scope the mere informative or study interests.

**FOCUS**

**The Progression of Repression Instruments in the Italian System**

● **Historical Phase (Original Art. 270 c.c.):** Focus centered on protecting the state personality and on internal associative crimes (e.g., subversive associations and armed bands of an internal political matrix).
● **Transnational Emergency Phase (Decree-Law 374/2001 – Art. 270-*bis* c.c.):** Extension of the associative offense to the international dimension. Configuration of the terrorist purpose also in case of attacks directed against foreign States or supranational organizations.
● **Advanced Prevention Phase (Decree-Law 7/2015 and subsequent reforms):** Anticipation of the punishability threshold to purely individual and preparatory behaviours. Incrimination of traveling abroad for terrorism purposes (*foreign fighters*), financing a single conduct, and self-training via telematic and encrypted channels.

## X. How do Europol, Eurojust, and the EPPO Coordinate Cross-Border Eversive Investigations?

Operational enforcement against eversive networks within the European Union demands a level of inter-institutional coordination capable of overcoming the traditional

fragmentation of national criminal investigations. The molecular nature of modern terrorism requires that information exchange occurs immediately and in a centralized manner.

The security architecture of the European Union articulates around three judicial and police pillars:

- **Europol:** Through the **European Counter Terrorism Centre (ECTC)**, it serves as the central hub for sharing tactical and strategic information, monitoring financial flows and online propaganda. Furthermore, it annually publishes the *TE-SAT* report on terrorism situation and trends in the EU based on data from Member States. In 2021, a comprehensive decrease in arrests was recorded (388 compared to 449 in 2020), with a clear prevalence of investigations into jihadist terrorism (260 arrests concentrated in France, Spain, and Austria) and an increase in arrests related to right-wing extremism, contrasted by a decline in anarchist-insurrectionalist terrorism.
- **Eurojust:** Coordinates criminal prosecution among the national judiciaries of Member States, facilitating the transmission of evidence and the simultaneous management of arrest warrants. In 2019, Eurojust established the **Counter-Terrorism Register (CTR)**, a centralized database that collects in real time information on criminal proceedings and convictions for terrorist offenses across the Union, allowing for the detection of hidden links between parallel investigations and files.
- **EPPO (European Public Prosecutor's Office):** Although the original competence of the EPPO is focused on financial crimes harming the financial interests of the Union (Regulation EU 2017/1939), the Office coordinates its action in cases where complex fiscal fraud, smuggling, or money laundering are exploited or managed by eversive cells for the **autonomous financing of terrorism**.

To understand how these pillars interact in practice, the coordinated action against terrorism can be summarized in three consequential phases:

- **Interception Phase (Europol - ECTC):** Monitoring of the telematics network, tracking of anomalous financial flows, and publication of TE-SAT statistics to guide enforcement actions across the territory.
- **Data Matching Phase (Eurojust - CTR):** Insertion of judicial data into the Counter-Terrorism Register. Automatic detection of cross-border connections between files from different prosecutor's offices.

**Operational Phase (National Prosecutor's Offices / Investigation Squads):** Coordinated execution of searches, asset seizures, and simultaneous arrests through the use of the European Arrest Warrant (EAW) and the European Investigation Order (EIO).

**CASE STUDY**

**Court of Justice of the European Union, PNR, 2022**

An essential jurisprudential pillar is the judgment of the Court of Justice regarding Directive (EU) 2016/681 on the use of passenger name record (**PNR**) data. Called upon to assess the legality of the bulk collection of air travellers' data, the Court validated the Directive, recognizing its absolute necessity for the prevention of international terrorist crimes and the tracking of foreign fighters. However, in line with the orientation of protecting fundamental rights, the CJEU established that the application of the PNR system must be **limited to what is strictly necessary**, banning the use of predictive algorithms based on discriminatory profiles and requiring that the automated processing of data always be subject to effective human review before proceeding to stops or searches at the border.

## XI. Key Findings

The scientific and regulatory analysis carried out within this paper leads to the outline of **five fundamental findings**:

- **Dogmatic transition of the phenomenon:** The attacks of September 11, 2001, and the rise of global asymetric organizations such as **ISIS** (characterized by a utopian-territorial propaganda compared to the nihilism of *Al-Qaeda*) imposed a progressive recognition of international terrorism. Traditionally confined to the category of transnational crimes subject to purely domestic enforcement, the phenomenon has assumed the characteristics of an **international crime** that attacks the peace, collective security, and fundamental rights of the global community.
- **Relevance of specific intent in the definition:** In the absence of a unified global comprehensive international convention (hindered by political tensions surrounding the principle of self-determination of peoples), European law (Directive EU 2017/541, which updated Framework Decision 2002/475/JHA) defines the offense of terrorism through the mandatory concurrence of two elements: an **objective material element** (the commission of intrinsically serious acts) and a **qualified subjective element (specific eversive intent / *dolo specifico*)**, aimed at intimidating the population or unduly coercing the will of a State or an international organization.
- **Anticipation of the punishability threshold (Advanced prevention):** The multilevel legal response (UN, Council of Europe, European Union, and Italian risiones *ex* Art. 270-*bis* c.c. and following) has progressively abandoned the purely *ex-post* repressive logic. Safeguarding security has dictated the **autonomous criminalization of individual preparatory acts**, punishing instrumental conducts prior to the execution of the attack, such as recruitment, logistical training (Warsaw Convention 2005), and **online telematics self-training** (Law 146/2006 and anti-terrorism reforms).
- **Subsidiary role of Artificial Intelligence and administrative limits:** Countering digital radicalization relies on automated systems based on Artificial Intelligence (*Natural Language Processing* and *Image Matching* techniques). Where the vagueness of messages prevents criminal prosecution in compliance with the principle of specificity, legal systems resort to **immigration law and ministerial expulsions** for security reasons, balancing State protection with the

procedural guarantees established by the jurisprudence of the ECtHR (the *H.F. v. France* case on the limits to the right of return).

- **Consolidation of the mutual recognition model:** Operational coordination within the Area of Freedom, Security, and Justice relies on the interoperability of special agencies (Europol, Eurojust) and the use of the **Counter-Terrorism Register (CTR)**. The effectiveness of the European counter-terrorism system depends on bypassing the political filters of national governments and applying mechanisms for the mutual recognition of evidence and arrest warrants (the PNR system), balanced by the absolute respect for fundamental rights established by the Court of Justice of the EU (*Kadi* judgment).

# Transnational Organized Crime

*by Alessandra Giordano and Miriana Greco*[*]

SUMMARY: I. Why Does Transnational Organized Crime Constitute a Structural Threat to Internal Security? – II. Does A Definition of Transnational Organized Crime Exist? – III. Which Criteria Determine the Transnational Nature of an Offense According to the United Nations Convention Against Transnational Organized Crime (UNTOC)? – IV. What Legislative Instruments Have Been Adopted to Harmonize Cross-Border Core Offenses? – V. What Is the Role of The UNTOC Open Clause in Countering Emerging Crimes? – VI. How Has the Transnational Offense Framework Been Integrated into Domestic Law? – VII. Which Special Investigative Techniques Are Provided by Italian Legislation to Counter Transnational Networks? – VIII. What Is the Structural Difference Between the Historical Institution of Extradition and The European Arrest Warrant (EAW)? – IX. What Role Do Asset Recovery and the Confiscation of Illicit Proceeds Play in the Global Anti-Mafia Strategy? – X. How Do Specialized Agencies Coordinate Field Strategies Through the UNODC Digest?

KEY FINDINGS: Affirmation of Intelligence-Led Policing; Definitional flexibility of the open clause; Inadequacy of isolated responses; Strategic centrality of asset recovery; Transition from a political to a judicial model.

## I. Why Does Transnational Organized Crime Constitute a Structural Threat to Internal Security?

Transnational organized crime (**TOC**) no longer constitutes an emergency restricted within single national borders, but represents a **structural challenge of global interest**, capable of destabilizing the international political and economic order. Modern mafia cartels operate as true **multinational criminal corporations**, equipped with massive financial resources, interconnected logistical structures, and a distinct operational fluidity. This evolution jeopardizes the internal security of the Member States of both **the Council of Europe** and the **European Union**, acting on three destructive levels:

- **Erosion of the Rule of Law**: Through corruption and the systemic intimidation of public institutions, police forces, and the judiciary.
- **Infiltration of the Legal Economy**: The laundering of illicit capital distorts free competition, pollutes healthy commercial markets, and undermines the integrity of the European single market.

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

- **Violation of Human Rights**: The use of violence and the exploitation of social vulnerabilities (as seen in trafficking) directly strike the core values protected by the European Convention on Human Rights (ECHR).

**FOCUS**

**Effects of Digitalization**

In the current geopolitical scenario, criminal organizations have capitalized on the structural vulnerabilities and rapid digitalization accelerated by the post-pandemic transition. Transnational cartels have diversified their profit lines, adapting rapidly to global markets. Among the **emerging crimes with high social alarm**, the following are recorded:

- **Structured cybercrimes** and large-scale ransomware attacks against critical infrastructures.
- **Advanced computer fraud** and offenses related to digital identity theft.
- **Environmental crimes (*ecocrimes*)**, with particular reference to the illicit disposal of toxic waste.
- **Transnational commercialization** of counterfeit medicines, vaccines, and medical devices.
- **Illicit trafficking** of precious goods, conflict minerals, and looted artworks.

## II. Does A Definition of Transnational Organized Crime Exist?

The doctrinal debate has long struggled to find a unanimous consensus: while traditional Italian doctrine tended to identify the phenomenon exclusively around the rigid criteria of the structured mafia model, the international and Euro-unitarian orientation prefers an **objective and flexible** qualification, suitable for targeting fluid criminal networks that lack a historical or territorial root.

The universal dogmatic synthesis was codified by the **United Nations Convention against Transnational Organized Crime** (known internationally by the acronym **UNTOC** or as the *Palermo Convention* of 2000), a framework subsequently transposed also within the European Union's **Framework Decision 2008/841/JHA**.

According to Art. 2 of UNTOC an "'**organized criminal group**' shall mean a structured group, consisting of **three or more persons**, existing for a period of time and acting in concert with the aim of committing one or more **serious crimes**, punishable by a maximum deprivation of liberty of **at least four years**, in order to obtain, directly or indirectly, a **financial** or other material benefit"

To facilitate memorization, the **constitutive elements** established by UNTOC that we must remember are:

- **The numerical criterion**: Presence of a minimum number of **three or more people**.
- **The temporal element**: It must be a structured group that has **existed for a period of time**, excluding mere occasional association for a single offense.
- **The economic purpose**: The ultimate goal of the activity must consist in obtaining financial **or other material benefits**.
- **The gravity threshold**: The common action must be oriented toward the commission of offenses punishable by a maximum reclusion of **not less than four years** (*serious crimes*).

The multilevel regulatory articulation (the governance of the contrast) is composed of:

- **International level (UN)**: United Nations Convention (**UNTOC 2000**). Focus centered on the **global definition of a structured group** and on the establishment of international obligations for incrimination and assisted confiscation.
- **Regional level (Council of Europe)**: Recommendation **Rec(2001)5**. Provides common monitoring standards for national criminal policies and guarantees the constant **balancing of measures with the Human Rights** of the ECHR.
- **European level (European Union)**: Framework Decision **2008/841/JHA**. Introduces the **harmonization of minimum criminal penalties** within the area of freedom, security, and justice, activating the **EMPACT** operational platform.
- **National level** (Italy): National System (**Law 146/2006**). Implements the transposition of treaties by introducing the legal figure of the **Transnational Offense** and coordinating it with the special offense of mafia association *ex* **Art. 416-*bis*** of the Criminal Code.

## III. Which Criteria Determine the Transnational Nature of an Offense According to the United Nations Convention Against Transnational Organized Crime (UNTOC)?

The notion of **transnationality** is fundamental. It does not simply coincide with the physical crossing of a geographical border by the offender but invests the entire **logistical and executive planning** of the criminal action. It is the ascertainment of this cross-border dimension that legitimizes the activation of international cooperation instruments. According to para. 2 of the provision, an offense is transnational in nature if:

- It is committed in more than one State;
- It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
- It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
- It is committed in one State but has substantial effects in another State.

**CASE STUDY**

**Italian Cassation Court, Judgment No. 4307, 2024**

"For the purpose of configuring the aggravating circumstance of transnationality, it is indispensable to ascertain that the offense was planned, facilitated, directed, or consummated, at least in a relevant or substantial part, abroad, requiring a causal link between transnationality and the activity of the organized group."

With this fundamental ruling, the Italian Supreme Court of Cassation clarified the boundaries of national jurisdiction by examining a case of cross-border commercial fraud. The judges ruled that transnationality requires **rigorous evidentiary verification** regarding the logistical elements located across the border. This interpretative strictness has the practical effect of **preventing the pretextual or automatic use of the aggravating circumstance** for entirely domestic crimes, safeguarding the principle of specificity in criminal law.

## IV. What Legislative Instruments Have Been Adopted to Harmonize Cross-Border Core Offenses?

Differences between the criminal codes of various States historically represent the main obstacle to the effectiveness of investigations. The universal regulatory pillar to overcome

this fragmentation is the **United Nations Convention against Transnational Organized Crime (UNTOC)**, adopted by the General Assembly on November 15, 2000, through Resolution 55/25.
UNTOC operates by imposing on signatory States the **mandatory introduction** into their respective domestic criminal laws of **four core offenses**:

1. **Participation** in an organized criminal group (Article 5).
2. **Laundering** of proceeds of crime (Article 6).
3. **Corruption** of public officials (Article 8).
4. **Obstruction of justice** (Article 23).

**FOCUS**

**The Supplementary Protocols to the UNTOC**

The UNTOC Convention is structurally integrated by **three targeted Protocols**:

- **Protocol on Trafficking in Persons**: Centred on the prevention, suppression, and punishment of the exploitation of human beings, with particular attention to the protection of women and children, and on the international protection of victims (in force since December 25, 2003).
- **Protocol against the Smuggling of Migrants by Land, Sea, and Air**: Aimed at targeting the facilitation of illegal immigration managed for profit by trafficking networks (in force since January 28, 2004).
- **Protocol against the Illicit Manufacturing of and Trafficking in Firearms**, Their Parts, Components, and Ammunition: Adopted through Resolution 55/255 to facilitate cross-border tracking and the exchange of ballistic data (in force since July 3, 2005).

The **Council of Europe** intervenes in this scenario by integrating the repressive dimension with that of the **protection of fundamental rights**, guaranteeing through the jurisprudence of the **ECtHR** that special anti-mafia regulations do not violate the guarantees of a fair trial (**Article 6 ECHR**) or the right to property (**Article 1, Protocol 1 ECHR**) in cases of seizure.

## V. What Is the Role of The UNTOC Open Clause in Countering Emerging Crimes?

The intrinsic strength of UNTOC lies in its nature as a "**living treaty**" capable of evolving. The authors of the UN Convention deliberately chose not to insert a rigid and closed list of punishable offenses, because criminal markets and technologies change with extreme rapidity.
The Convention applies to an open list of emerging crimes thanks to the **general clause** contained in **Art. 2, letter b) of UNTOC**, which defines a **"serious crime"** as any offense punishable by a maximum deprivation of liberty of **at least four years**. This flexible extension covers today:

- **Cybercrime**, supporting the cross-border acquisition of digital evidence.
- **Environmental crime**, aimed at countering the illicit trafficking of hazardous waste and protected species.
- **International trafficking of cultural property** and the falsification of medical and healthcare products.
- Offenses related to **international terrorism**, where funding through mafia channels is established.

Thanks to this mechanism, resolutions of the **Conference of the States Parties (COP)** can constantly extend the application of UNTOC's assistance tools (such as extradition and mutual assistance) to emerging phenomena of computer crime and *ecocrimes* without having to draft new treaties.

## VI. How Has the Transnational Offense Framework Been Integrated into Domestic Law?

Italy gave full execution to the Palermo Convention through **Law No. 146 of March 16, 2006**. The national legislator made a precise technical choice: it did not create an autonomous figure of crime called a "transnational felony" but configured transnationality as a **common aggravating circumstance with special effect**.
The **four pillars** of **Law 146/2006** that we must memorize are:

- **The internal definition (Article 3)**: An offense is transnational if it is punishable by reclusion of no less than four years in its maximum, committed by an organized criminal group, and involves more than one State.
- **The special aggravating circumstance (Art. 4, today Art. 61-*bis* of the Criminal Code)**: Entails a mandatory increase of sentence **from one-third to one-half** for crimes committed by taking advantage of or in order to facilitate a transnational organized group.
- **Liability of Entities (Legislative Decree 231/2001)**: Art. 10 of Law 146 inserts transnational offenses into the catalogue of core offenses that generate **administrative and patrimonial liability for corporate companies**.
- **Extension of anti-mafia protections**: Investigations for crimes aggravated by transnationality are delegated to the exclusive competence and special investigative functions of the **District Anti-Mafia Directorate (DDA)**.

**CASE STUDY**

**Italian Cassation Court, Second Penal Section, Judgment No. 27379, 2023**
"The special aggravating circumstance of transnationality, provided by Art. 61-*bis* of the Criminal Code, has an objective nature and extends to co-conspirators who had knowledge of it or who ignored it through negligence, regardless of an actual conviction for the primary associative offense."
The Supreme Court addressed a case concerning the international smuggling of manufactured tobacco managed by a cell operating between Eastern Europe and Italy. The defense argued that the aggravating circumstance was inapplicable because the defendant was external to the main criminal association. The judges of legitimacy rejected the appeal, ruling that **transnationality applies to the single specific crime** provided the co-conspirator was fully aware that they were facilitating a structured organization operating on an international scale.

## VII. Which Special Investigative Techniques Are Provided by Italian Legislation to Counter Transnational Networks?

Traditional reactive investigation tools are ineffective against criminal organizations protected by sophisticated encrypted communication systems and jurisdictional barriers. For this reason, the Italian system, transposing the provisions of Art. 20 of the UNTOC Convention, has codified exceptional instruments of procedural derogation.

**Article 9 of Law 146/2006** establishes a special **cause of justification** (non-punishability) for judicial police officers who perform acts that would abstractly constitute an offense, for the sole purpose of acquiring stable evidence. The special investigative techniques permitted by Art. 9 are:

- **Undercover Operations**: Controlled infiltration of State agents into criminal networks to acquire evidence and information from within the clans. The acts performed by the agents (such as simulating the purchase of weapons or drugs) are protected by a cause of exclusion of criminal liability.
- **Controlled Deliveries**: Provide for the deferral of the seizure of illicit goods, narcotic substances, or counterfeit currency. Through the constant monitoring of the transit of shipments across national borders, the objective shifts from secondary couriers to identifying the real leaders and final destinations of the network.

**FOCUS**

**Operational Derogations *ex* Art. 9 Law 146/2006**

The two operational techniques allow the judicial police to act proactively. Delaying the seizure or the arrest of couriers (*delayed seizure*) is the fundamental tool to avoid the premature interruption of a cross-border investigation, guaranteeing the collection of stable legal evidence usable in trial against the leaders located abroad.

## VIII. What Is the Structural Difference Between the Historical Institution of Extradition and The European Arrest Warrant (EAW)?

The study of the evolution of mechanisms for surrendering wanted persons highlights the transition from an ancient system of diplomatic relations to a modern model of integrated judicial cooperation.

The comparative analysis articulates around two diametrically opposed models:

- **Traditional Extradition**: Qualifies historically as an **act of sovereignty and political courtesy** between States. The procedure is cumbersome, suffers from long execution times, and is dominated by the **discretionary filter of the Executive Power** (Ministry of Justice), which can refuse the surrender of the wanted person to safeguard national political interests. Legal nature: Act of courtesy and political sovereignty between sovereign States. Transmission channel: Diplomatic and ministerial, with strong government discretion. Operational characteristics: Complex, cumbersome procedure characterized by long timeframes.
- **The European Arrest Warrant (EAW)**: Introduced by **Framework Decision 2002/584/JHA**, completely erases the political filter and configures itself as an **enforceable judicial decision** based on the cornerstone principle of **mutual recognition**. The exchange takes place directly and exclusively between the judicial authorities (Prosecutor's Offices and Courts of Appeal) of the Member States of the European Union, within **strict mandatory time limits** (maximum 60 days). Legal nature: Directly enforceable judicial decision within the common legal area. Transmission channel: Direct judicial channel between Prosecutor's Offices and Courts of Appeal, without political filters. Operational characteristics: Standardized, simplified procedure characterized by distinct rapidity.

**CASE STUDY**

**Court of Justice of the European Union, C.J., 2025**

"The execution of a European arrest warrant may not be refused except for reasons exhaustively provided for. However, the executing judicial authority must decide to postpone the surrender if there is a real risk of violation of Art. 4 of the Charter of Fundamental Rights related to the conditions of detention in the issuing Member State."

**Court of Justice of the European Union, Rugu and Aucroix, 2026**

In the cases of *Rugu* and *Aucroix* of June 2026, the Court of Justice had to resolve a conflict between the obligation of rapid surrender of an organized crime broker and the protection against degrading treatment. The Court ruled that the executing State must urgently request supplementary information from the issuing State and, only in the absence of suitable guarantees on the prison regime, may postpone the surrender, **balancing the principle of mutual recognition with the fundamental rights of the person**.

## IX. What Role Do Asset Recovery and the Confiscation of Illicit Proceeds Play in the Global Anti-Mafia Strategy?

Modern criminology highlights how transnational organized criminal groups are driven by a single motivation: the accumulation of economic profit and the **accumulation of wealth**. Consequently, the penal sanction of imprisonment is insufficient if not accompanied by the **financial dismantling of the clan**. Confiscation transforms from a mere additional penalty into a **strategic preventive tool**.

**REFERENCES**

**UNTOC, 2000, Art. 12 and Art. 13**

"Each State Party shall adopt such measures as may be necessary to enable confiscation of proceeds of crime derived from offenses covered by this Convention or property the value of which corresponds to that of such proceeds, as well as property, equipment or other instrumentalities used in or destined for use in the commission of offenses."

The Italian system stands at the global forefront in this sector, having implemented – in harmony with Art. 11 of Law 146/2006 – the institution **of value confiscation (confiscation by equivalent)**. If it is not possible to trace the direct and specific profit of the transnational offense, the judge orders the seizure and confiscation of sums of money, movable or immovable property, or other assets of a **value proportional to that in the offender's availability**, directly targeting the personal assets accumulated unlawfully.

## X. How Do Specialized Agencies Coordinate Field Strategies Through the UNODC Digest?

Institutions coordinate their action on the field by combining doctrinal analysis with operational activity. Following the recommendations issued by the Conference of the States Parties to UNTOC in 2010, Italy led the drafting of the **"Digest of Organized Crime Cases**" (published in collaboration with UNODC in 2012). The Digest empirically demonstrated that international investigations succeed only if action focuses on the **structural dismantling of the network**, rather than on the single specific crime.

**FOCUS**

**"Operation Giotto" Investigation**

Italian investigation conducted by the Carabinieri (UNODC reference classification: **ITA18**).

- **Legal issue**: Ascertain the existence of a single transnational associative structure with a top-down and polycentric character, capable of operating in Italy, France, Spain, and Germany for the production and commercialization of counterfeit banknotes.
- **Applied law**: Art. 416 of the Criminal Code coordinated with the aggravating circumstance of transnationality *ex* **Art. 3 of Law 146/2006** and the use of special investigative techniques of **Art. 9** of the same law.
- **Operational analysis**: The investigation proved that the 11 territorial cells constituted a true criminal consortium. Investigators monitored financial flows across borders, exchanging data in real time with the involved foreign authorities, bypassing national barriers through **Europol** (criminal intelligence analysis), **Eurojust** (prosecutorial coordination), and **OLAF** (fight against customs fraud).
- **Judicial outcome**: Dismantling of the cartel, arrest of over 170 people including top leaders, and seizure of massive illegal printing facilities. Inserted in the UNODC Digest as an operational model for coordinated investigations.

The general summary matrix (alignment for proceedings) in synthesis is:

- **Global cooperation: UNTOC Convention (Palermo 2000)**. Structural identification of the organized group. It constitutes the legal basis for extending enforcement to modern cybercrimes and ecocrimes.
- **Italian transposition: Law 146/2006**. Aggravating circumstance of transnationality and targeted reforms to the Criminal Code. Extension of special powers and attributions of the District Anti-Mafia Prosecutor.
- **Case analysis: UNODC Digest (Giotto Case)**. Study of a structured network with a hierarchical and consolidated character. Key example of coordinated investigations between foreign police forces.
- **Intelligence exchange: EU - INTERPOL Partnership**. Interoperability of security databases. Direct access through the European portal to global databases **SLTD** (stolen documents) and **TDAWN** (capture alerts).

**FOCUS**

**The EMPACT Operational Cycle (2026-2029)**

Based on the conclusions adopted by the Council of the European Union, the new permanent **EMPACT cycle for the period 2026-2029** directs investigative efforts toward the dismantling of high-risk criminal networks in Europe, known as **Most Threatening Criminal Networks and Individuals (MCTNI)**. This approach funds joint operational actions (*Action Days*) to counter high-priority crimes, such as environmental crime and human trafficking. In support of these measures, the European Union utilizes the **Internal Security Fund (ISF) for the period 2021-2027**, aimed at improving information sharing, intensifying cross-border cooperation, and elevating national technological capabilities of police forces in detecting computer and cryptographic traces.

The operational and financial architecture of the European Union in this area is made up of:

- **The EMPACT Operational Platform (Operational Cycle 2026-2029)**: Scope of action: Implementation of field strategies based on the *Intelligence-led policing* model. Priority focus: Targeted dismantling of high-risk networks (**MCTNI**) and

execution of coordinated *Action Days* on environmental crimes, trafficking, and counterfeiting.

- **The Internal Security Fund (ISF) Financial Instrument (Period 2021-2027)**: Information Sharing: Financial support for the interoperability of data systems of European agencies. *Cross-Border Cooperation*: Logistical funding for the establishment and mobility of **Joint Investigation Teams (JIT)**. *Capacity Building*: Funds allocated for the purchase of software and specialized forensic technical training to decrypt digital traces and cryptocurrencies used by clans.

## XI. Key Findings

The scientific analysis carried out within this paper leads to the outline of **five fundamental findings** that we must assimilate for a complete understanding of the phenomenon:

- **Inadequacy of isolated responses**: Transnational organized crime (**TOC**) acts on the market as a structured and de-localized network. Consequently, the isolated action of a single State is anachronistic and ineffective. Countering it necessarily requires **integrated multilevel cooperation** between the UN, the Council of Europe, the European Union, and individual national criminal systems.
- **Definitional flexibility of the open clause**: Based on the architecture of the **UNTOC** Convention, the effectiveness of assistance tools is not bound to a rigid catalogue of offenses. On the contrary, the use of the clause of *serious crimes* (offenses with a maximum penalty of four years or more) allows for the immediate extension of protections and coordinated investigations to emerging technological threats, such as **cybercrimes** and **environmental crimes**.
- **Transition from a political to a judicial model**: The evolution of mechanisms for surrendering wanted persons demonstrates the success of the principle of **mutual recognition**. The transition from traditional extradition (cumbersome and dominated by the political discretion of governments) to the **European Arrest Warrant (EAW)** has judicialized the exchange between Prosecutor's Offices, reducing surrender times to a strict maximum of 60 days.
- **Strategic centrality of asset recovery**: Modern anti-mafia strategies go beyond the logic of mere custodial sanctions, focusing on the economic principle of *follow* the money. Targeting illicit wealth through proactive measures and advanced institutions such as **value confiscation** constitutes the most effective preventive tool to block the destabilization of healthy commercial markets.
- **Affirmation of Intelligence-Led Policing**: European strategic lines of action are shifting toward proactive prevention. Through the interoperability of security databases and the **EMPACT** operational cycle, the common effort is no longer aimed at fragmentarily striking the single crime, but at **systematically dismantling high-risk criminal networks (MCTNI)** operating in the Euro-unitarian area.

# Human Trafficking and Sexual Exploitation of Women and Minors

*by Orsola Ilenia Conte*[*]



KEY FINDINGS: A vigorous and stringent international, European, and national regulatory response; Human trafficking is a growing transnational crime; Italy and anti-trafficking mechanisms; Smuggling of migrants and trafficking in persons; Frequently blurred boundaries; The prevalent form of trafficking is the sexual exploitation of women and minors; The use of digital technologies has transformed the landscape of human trafficking.

## I. What Are the Identifying Elements of The Crime of Trafficking in Human Beings?

Trafficking in human beings is a complex transnational crime, defined by most as a modern form of "slavery." It is a criminal activity aimed at the capture, abduction, or recruitment, as well as the transportation, transfer, harboring, or receipt of one or more persons, using illicit means and for the purpose of exploiting them. More precisely, Art. 3 of the Palermo Protocol (Protocol supplementing the United Nations Convention against Transnational Organized Crime, 2000) provides the following legal definition of trafficking:

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

**REFERENCES**

**Trafficking in Persons Protocol supplementing the UNTOC (2000), Art. 3 para. a** "the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs."

In practice, traffickers impose their will on the victims, exploiting their helplessness and employing means of pressure (deception, threats, violence) against vulnerable individuals who find themselves in difficult life situations. This position of vulnerability implies that the victim has no real or acceptable alternative but to submit to the abuse. Trafficking can occur both across national borders and within the same country and constitutes, in addition to being a serious violation of human rights, a genuine global public safety issue. Historically, the prohibition of slavery is numbered among the oldest in customary international law (jus cogens). Indeed, a Declaration concerning the abolition of the slave trade dates back to 1815, followed by numerous international treaties and conventions on the matter. Among these, the following are noteworthy: the 1949 Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others; the aforementioned 2000 Palermo Protocol; and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000).

At the European level, the cornerstone is the **Council of Europe Convention on Action against Trafficking in Human Beings (Warsaw, 2005)**. Within the European Union context, the regulatory framework has been recently strengthened by **Directive (EU) 2024/1712**, which amended the historic Directive 2011/36/EU, and by **Directive (EU) 2024/1385** on combating violence against women and domestic violence. These latest provisions have introduced stricter criminalization at the European level, extending protections for victims and explicitly including forced marriages and illegal adoptions among the forms of exploitation.

**In Italian domestic law**, the relevant regulatory profiles are found in **Art. 600 (Reduction to or maintenance in slavery or servitude) and Art. 601 (Trafficking in persons) of the Criminal Code**, which were deeply reformed to align with international obligations. The Italian legal system is characterized by the so-called "integration model" between criminal prosecution and social protection, regulated by **Art. 18 of the Consolidated Law on Immigration (Legislative Decree 286/1998)**. This provision grants a special residence permit for social protection reasons to victims fleeing criminal networks, regardless of their cooperation in the criminal proceedings. Strategic coordination is entrusted to the "National Action Plan against trafficking and serious exploitation of human beings".

From a social and cultural context perspective, this form of transnational crime finds fertile ground in realities characterized by poverty, sharp social inequalities, fragile local institutions, inefficient judicial systems, high rates of corruption, and the uncontrolled proliferation of civil wars. Women and minors are undoubtedly the most vulnerable subjects due to the predominance of patriarchal values, the commodification of the female body, and their sexuality. Furthermore, the purposes of trafficking and exploitation differ

significantly based on gender: men are mainly employed in the construction, agricultural (*caporalato*), and industrial sectors, while women and female minors are predominantly destined for sexual exploitation and forced domestic work.
Trafficking in human beings is a serious crime against the person and consists of three constituent elements:

1. **The conduct**: the recruitment, transportation, transfer, harboring, or receipt of persons.
2. **The instrument**: the use of force, coercion, abduction, fraud, deception, or the abuse of a position of vulnerability.
3. **The purpose**: exploitation (sexual exploitation, forced labor, slavery, organ removal, or forced illegal economies).

All of this translates into an aberrant violation of human rights, as it involves reducing a person to a mere commodity, deprived of their freedom and dignity. Victims are forced to live in conditions of slavery with no possibility of choice or escape, subjected to continuous physical and psychological violence. In many cases, traffickers enjoy impunity due to the transnational nature and fluid structure of criminal networks, which complicates the identification of the abusers and the gathering of evidence.

**REFERENCES**

**Universal Declaration of Human Rights,1948 , Art. 4**
"No one shall be held in slavery or servitude; slavery and the slave trade shall be prohibited in all their forms".

## II. How Do the Different Forms of Trafficking Manifest?

The primary purpose of trafficking is the economic and personal exploitation of the victim, which can take various forms:

- **Trafficking for sexual exploitation**: predominantly involves women, adolescents, and young girls who are forced into prostitution or subjected to abuse in physical or virtual circuits under the control of traffickers.
- **Trafficking for forced labor**: victims are compelled to work under inhumane conditions, under threat, often without remuneration or to settle artificial debts (debt bondage), especially in agriculture, construction, domestic work, and the hospitality sector.
- **Trafficking for forced begging**: minors or highly vulnerable individuals (persons with disabilities, the elderly) are forced to beg in public areas; the earnings are entirely confiscated by criminal networks, depriving them of their freedom and means of survival.
- **Trafficking for illegal adoptions**: consists of illicitly obtaining infants or children for adoption, bypassing national and international legal procedures, often tearing them from their families of origin through deception, coercion, or financial transactions.
- **Trafficking for forced marriages**: young women or minors are convinced or forced to leave their homes with promises of work or a better future, only to be sold for marriage purposes, facing isolation, abuse, and chronic domestic and sexual exploitation.

• **Trafficking for organ removal**: victims are deceived, threatened, or forced to undergo organ harvesting in clandestine and life-threatening environments. The organs are then illegally sold on the global black market for transplants.
• **Trafficking for forced criminal activities**: victims are obliged to commit offenses (thefts, pickpocketing, drug trafficking, or cultivation of illegal crops) under the direction and for the exclusive profit of criminal organizations.

Although these various forms target different illicit markets, they present a common matrix: the methods of coercive and psychological control used by traffickers to subjugate victims. Traffickers do not only rely on physical confinement; they use psychological manipulation, threats of retaliation against family members in the countries of origin, substance addiction, and the exploitation of travel debts. Due to economic precariousness, lack of knowledge of the local language and laws of the transit or destination country, and fear of deportation by immigration authorities, it is extremely difficult for victims to seek help, defend themselves, or report the exploitation.

Since trafficking is a hidden phenomenon that develops predominantly in the shadows, estimating the precise number of victims is complex. Data is aggregated through reports from law enforcement agencies, NGOs, and international institutions that monitor the progress of investigations and the protections provided.

• **The Transformation of Cyber-trafficking**: Today, human trafficking has undergone a profound digital transformation, evolving into so-called cyber-trafficking. Digital technologies act as a powerful multiplier and facilitator of crime at every stage of the criminal business model. Traffickers utilize social media and job advertisement platforms to target vulnerable individuals (e-hunting). Furthermore, sexual exploitation has partially moved online through live streaming on encrypted platforms and monetization via cryptocurrencies (such as Bitcoin), which guarantee the anonymity of financial flows and complicate asset tracing by law enforcement.

**FOCUS**

**United Nations Office on Drugs and Crime – Global Report on Trafficking in Persons, 2024**

The **Global Report on Trafficking in Persons** published by the United Nations Office on Drugs and Crime highlights that impunity for trafficking offenses remains high globally. At the same time, it records an alarming growth in trafficking cases linked to the misuse of digital platforms and an increase in the involvement of minors within cyber-trafficking networks.

## III. What International Instruments Have Been Adopted to Suppress Trafficking in Persons?

International law has developed multiple regulatory instruments to combat human trafficking, with the shared objective of providing a solid legal basis for transnational repression and the protection of victims.

- **Universal and Conventional Level**: The global pillar is the **Palermo Protocol** supplementing the United Nations Convention against Transnational Organized Crime (UN, 2000). The Protocol establishes the **irrelevance of the victim's consent** whenever force, coercion, or deception has been used. It imposes

legislative and operational obligations on signatory States, urging them to also address the structural factors (poverty, underdevelopment) that feed vulnerability. For the protection of minors, this framework is integrated by the **Convention on the Rights of the Child (New York, 1989)** – which rejects all forms of economic and sexual exploitation under the principle of the best interest of the child – and the **International Labour Organization (ILO) Convention No. 182 (1999)** on the worst forms of child labor. Trafficking is thus configured as a violation of human rights guaranteed by customary norms (jus cogens) and by fundamental treaties such as the UN Covenant on Civil and Political Rights, the ECHR, the American Convention, and the African Charter on Human and Peoples' Rights.

- **European and Domestic Law Profiles**: At the European regional level, the **Council of Europe Convention on Action against Trafficking (Warsaw, 2005)** and **Directive 2011/36/EU** (updated by Directive EU 2024/1712) bind Member States to high standards of incrimination and assistance. The Italian legal system responds to these obligations through **Art. 600 and Art. 601 of the Criminal Code**, which severely punish reduction to slavery and trafficking, supported by **Art. 18 of Legislative Decree 286/1998 (Consolidated Law on Immigration)**. The latter is a vanguard model that grants a residence permit for social protection reasons regardless of whether the victim cooperates in the criminal proceedings. Strategic coordination is managed through the "National Action Plan against trafficking and serious exploitation of human beings".
- **The Operational Countermeasures**: International enforcement can no longer ignore the digital dimension. Criminal networks leverage end-to-end encryption and hosting services in non-cooperative jurisdictions to manage sexual exploitation and launder proceeds. Conversely, international judicial cooperation (through agencies like Eurojust and Europol) utilizes advanced technological tools: secure cyber-cooperation platforms, the exchange of digital forensic data, and the use of Artificial Intelligence for predictive monitoring of opaque financial flows based on cryptocurrencies.

**CASE STUDY**

**European Court of Human Rights, S.M v. Croatia, 2020**

From a legal perspective, in international and European practice, there is no autonomous definition of sexual exploitation of women and minors, which has traditionally been subsumed within the scope of human trafficking. The landmark judgment **S.M. v. Croatia (Grand Chamber of the ECtHR, June 25, 2020)** marked a turning point, proposing a disarticulation of the notion of sexual exploitation for the purpose of prostitution from that of trafficking in human beings. The Court brought both offenses – even when the exploitation is not linked to a trafficking transaction – within the scope of application of **Art. 4 of the ECHR** (prohibition of slavery and forced labor), delineating an important development in the interpretative evolution of the norm.

## IV. How Does Trafficking in Human Beings Differ from the Smuggling of Migrants?

Trafficking in human beings and the smuggling of migrants constitute two distinctly different criminal offenses, although they are characterized by frequent operational points of contact.

- **Nature of the Crime and Consent**: Trafficking is a **crime against the person**. It is composed of three elements (conduct, coercive/deceptive means, and the purpose of exploitation) and disregards the consent of the victim, which is coerced or vitiated. Conversely, smuggling is a **crime against the State** and public order (corresponding in Italy to the offense of "facilitating illegal immigration" under Art. 12 of the Consolidated Law on Immigration). It is based on a contractual and voluntary agreement between the migrant and the smuggler to illegally cross a border in exchange for a fee, without any purpose of subsequent exploitation.
- **Transnationality and Borders**: Smuggling is by its very nature an inherently **transnational crime**, as it strictly requires the crossing of an international border. Trafficking, on the other hand, pursuant to the Palermo Protocol, can also be configured as a **domestic offense** (internal trafficking), developing entirely within the borders of a single State without the victim ever crossing a frontier.
- **The Intersections Between the Two Phenomena**: Digital technologies act as a catalyst and a point of intersection between the two crimes. Through so-called "tech-facilitated smuggling", smugglers use social media and digital payment systems (or digitized informal networks like *Hawala*) to plan migratory journeys. However, the line of demarcation is fluid: an individual who voluntarily resorts to smuggling can transform into a victim of trafficking during the journey or upon arrival. This occurs when criminals, abusing the migrant's irregular status and vulnerability, seize their digital documents or mobile devices, alter the terms of the original agreement, and subject them to blackmail, violence, or reduction to slavery for sexual or labor exploitation.

**REFERENCES**

**Trafficking and Smuggling**

| **Trafficking in persons** | **Smuggling of migrants** |
|---|---|
| Protocol to Prevent, Suppress and punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, Art. 3 (a). | Protocol Against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, Art. 3 (a). |
| "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs" | "the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident" |

## V. What Council of Europe Standards Monitor Trafficking and Sexual Exploitation?

At the regional continent level, the action of the Council of Europe is distinctly oriented toward the protection of human rights and a victim-centered approach.

- **The Warsaw Convention (2005)**: Compared to the 2000 UN Protocol, the **Convention on Action against Trafficking in Human Beings** shifts the focus from mere law enforcement to the protection of fundamental rights. The Convention dictates that victims must not be treated as irregular migrants, introducing the legal obligation of the "**recovery and reflection period**" (at least 30 days), during which they cannot be deported and receive material and psychological assistance to break free from the traffickers' influence. The effectiveness of the Convention is monitored by **GRETA** (Group of Experts on Action against Trafficking in Human Beings), an independent body that periodically evaluates the implementation by Member States and issues binding recommendations.
- **The Lanzarote Convention (2007)**: Specifically focused on the protection of children against sexual exploitation and sexual abuse, this Convention requires States to criminalize severe conducts such as child prostitution, child pornography, child corruption, and **grooming** (the online enticement of children for sexual purposes).
- **Profiles of Domestic Law**: Italy ratified the Lanzarote Convention through **Law No. 172/2012**, introducing profound reforms to the Criminal Code: penalties for sexual offenses against minors were increased, and new autonomous offenses were introduced, including Art. 609-*undecies* of the Criminal Code (Child grooming). On the procedural side, the reform introduced safeguards to avoid secondary victimization, such as protected hearings for the minor in specialized facilities with the support of psychological experts.
- **The Technological Evolution**: The Council of Europe addresses the link between technology and exploitation by integrating these provisions with the **Budapest Convention on Cybercrime**. GRETA's monitoring highlights how traffickers currently use encryption and the Dark Web to evade controls. The most recent guidelines require States to strengthen digital forensic capabilities and financial investigations based on **blockchain forensics** to intercept the proceeds of human trafficking.

**CASE STUDY**

**European Court of Human Rights, Rantsev v. Cyprus and Russia, 2010**

In the judicial landmark case Rantsev v. Cyprus and Russia (2010), the European Court of Human Rights (ECtHR) ruled that trafficking in human beings, by its very nature and purpose of exploitation, falls directly within the scope of application of Art. 4 of the ECHR (Prohibition of slavery and forced labor). The Court emphasized that trafficking involves the exercise of powers akin to the right of ownership, treating human beings as commodities to be bought and sold, restricting their freedom of movement, and exploiting them through violence and threats, predominantly (but not exclusively) within the sex industry.

## VI. How Does the European Union Combat Trafficking and Sexual Exploitation?

The European Union addresses trafficking through an integrated criminal justice and security system, based on the principle of harmonizing the legislation of its Member States.

- **The Legal Basis (Art. 83 TFEU)**: The Treaty on the Functioning of the European Union explicitly lists trafficking in human beings and the sexual exploitation of women and minors among the "**Eurocrimes**" (Art. 83, para. 1, TFEU). This grants the European Parliament and the Council the competence to adopt directives establishing minimum rules concerning the definition of criminal offenses and sanctions, given the inherently transnational nature of these conducts.
- **Directive 2011/36/EU**: This represents the cornerstone act on the matter. It formally defines the **position of vulnerability** as a situation in which the person has no real or acceptable choice but to submit to the abuse, establishing the absolute **irrelevance of consent** to the exploitation whenever coercive or deceptive means are present. It imposes strict obligations for early identification, assistance, and support, decoupling protection from the requirement of a formal complaint.
- **Profiles of Domestic Law**: The Italian legal system transposed this framework through **Legislative Decree No. 24/2014**, redefining the boundaries of the offenses under Art. 600 and Art. 601 of the Criminal Code and extending them to the buying and selling of slaves and forced labor exploitation. Here, the aforementioned **Art. 18 of the Consolidated Law on Immigration** finds perfect application, guaranteeing food, housing, and social integration pathways for foreign victims.
- **The Role of Technology in Enforcement**: To strike at the illicit economy generated on the web, the EU promotes operational cooperation through **Europol and Eurojust**. Domestic police forces (such as the S.C.O. and the Postal Police in Italy) utilize big data analytics and centralized financial tracking systems to block digital payment channels and identify cross-border criminal networks operating through foreign servers.

**FOCUS**

**Europol's Joint Supervisory Board**

A critical profile in the fight against trafficking lies in the management and processing of personal data by investigative authorities. Europol's Joint Supervisory Body and the European Data Protection Supervisor (EDPS) have highlighted the need for rigorous harmonization in the exchange of sensitive victim data between police, the judiciary, and NGOs. Incorrect management or the unjustified repetition of digital and physical interrogations risks triggering secondary victimization, re-traumatizing the victim during the criminal proceedings (Cf. Recital 20, Directive 2011/36/EU).

**Directive (EU) 36, 2011, Recital 20**

"Victims of trafficking in human beings who have already suffered the abuse and degrading treatment usually connected with trafficking, such as sexual exploitation, sexual abuse, rape, slavery-like practices or the removal of organs, should be protected from secondary victimization and further trauma during the criminal proceedings. To this end, victims of trafficking in human beings should receive appropriate treatment based on their individual needs. Judicial and investigative procedures should be structured to minimize direct contact between the victim and the accused, using remote communication technologies such as videoconferences, and ensuring that questions regarding the victim's private life are strictly limited to what is necessary for establishing the facts."

## VII. What Innovations Did the Recent EU Directive 2024/1712 Bring to The Fight Against Human Trafficking?

With the recent **Directive (EU) 2024/1712** on trafficking in human beings, the European institutions amended certain provisions of Directive 2011/36/EU and updated the previous regulatory framework, adapting it to the evolution of different forms of exploitation and new information and communication technologies (ICT).

This revision introduces stricter and more rigorous enforcement measures, expanding the scope of offenses falling under trafficking to include cases of **forced surrogacy exploitation**, **forced marriages**, and **illegal adoptions**. Great importance is given to victim protection; under Art. 11, States must arrange the necessary measures so that victims receive "specialized assistance". They are called to establish National Referral Mechanisms (NREM) to swiftly detect, identify, and support victims in collaboration with active organizations in the sector, thereby creating cross-border referral contact points. National Rapporteurs or equivalent mechanisms (NREMs) are essential in assessing the outcomes of anti-trafficking actions.

Another relevant amendment consists of the introduction of a new offense that penalizes the **intentional use of services** provided by a trafficking victim, provided the user is aware of the exploitation. This common definition is functional to reducing demand and standardizing judicial activities across Member States.

**FOCUS**

**New Technologies**

During the legislative process, the European Commission proposed inserting a specific Art. 2-*bis* to explicitly state that trafficking offenses include acts committed through information and communication technologies (ICT). In the final text of Directive 2024/1712, a different legislative technique was preferred: the use of digital technologies for distributing, facilitating, or producing images, videos, or similar material of a sexual nature concerning the victim was codified as a **specific aggravating circumstance**. This determines a significant increase in penalties, highlighting the criminal disvalue of cyber-trafficking.

## VIII. How Does the EU Address Digital Technologies in Sexual Exploitation?

In recent years, forms of exploitation have evolved, and human trafficking, in particular, has increasingly shifted online. Furthermore, the conflict between Russia and Ukraine has significantly contributed to a massive exodus of women and children, creating new opportunities for criminal organizations. Criminal networks are highly flexible, fast-acting, and exploit geopolitical, economic, environmental, and social crises to increase their illicit profits by offering illegal services online.

According to the UNODC, online platforms make it easier for traffickers to anonymously target specific categories of individuals whom they deem particularly vulnerable and easily enticed. In this regard, noteworthy is the position of the Council of the European Union on the directive proposal presented by the Commission concerning the fight against child sexual abuse and exploitation and child sexual abuse material.

The proposal aims to amend Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, specifically adapting criminal law to the technological evolution of crime in light of new online modalities of sexual abuse. Compared to the text proposed by the Commission, the Council urged the inclusion of an explicit reference to "reproductions and representations" within the definition of child sexual abuse material, referencing so-called "**deepfakes**" or material generated by artificial intelligence. It also confirmed the necessity of criminalizing "**child grooming**" practices related to the enticement of minors for sexual purposes through digital means. The main innovations of the directive include expanding the scope of sexual abuse offenses, providing for harsher penalties, and strengthening the victim support system.

**The Technical Operational Response**: In terms of cyber enforcement, the European Union coordinates cross-border operations through **Europol and Eurojust**. Within the framework of the **EMPACT** platform, the postal and cyber police forces of Member States utilize advanced network scanning software, monitoring encrypted messaging channels (such as Telegram) and Dark Web forums. In Italy, the **C.N.C.P.O.** of the Postal Police operates in synergy with European guidelines and the Digital Services Act (DSA), requiring internet service providers (ISPs) to immediately remove illegal content and block abusive websites, while tracking opaque financial flows based on cryptocurrencies to target the money laundering hubs of criminal organizations.

## IX. What Legal Pathways Define the Criminalization of Trafficking Under Domestic Law?

In Italy, according to the Ministry of the Interior, human trafficking constitutes the third largest source of income for criminal organizations, following arms trafficking and drug trafficking. To counter this phenomenon, the Italian State has adopted a regulatory system that integrates criminal enforcement, victim protection, and international cooperation.
**Law No. 228 of August 11, 2003** ("Measures against trafficking in persons") reshaped Art. 600, Art. 601, and Art. 602 of the Criminal Code, concerning respectively the crimes of "reduction to or maintenance in slavery or servitude," "trafficking in persons," and "purchase and sale of slaves," for which penalties were significantly increased, reaching a maximum of twenty years. The new Art. 600 of the Criminal Code makes explicit reference to exercising powers over a person corresponding to those of the right of ownership and to reducing or maintaining a person in a state of continuous subjection, forcing them into labor or sexual performance, begging, or, in any case, performances involving exploitation. Subsequently, **Legislative Decree No. 24 of 2014** updated the norms by explicitly including organ harvesting among the forms of exploitation.
The 2003 law established the under the Presidency of the Council of Ministers, intended to finance assistance and social integration programs, as well as a special assistance program to ensure, on a transitional basis, adequate housing, food, and healthcare conditions for trafficking victims. On October 19, 2022, the Council of Ministers adopted the "National Action Plan against trafficking and serious exploitation of human beings for the years 2022-2025", in implementation of EU Directive 2011/36. The Plan defines a series of actions fundamentally aimed at raising awareness, prevention, detection, and social integration of trafficking victims, resting on four guidelines: **prevention** to improve knowledge of the phenomenon and means for early identification of the crime; **prosecution** of the crime through the dismantlement of criminal structures and judicial cooperation; **protection** through suitable instruments to safeguard victims, especially women and children; and **cooperation** between States with integrative and supportive actions.

- **The Cyber Investigations**: To fully implement the National Action Plan, Italian District Anti-Mafia Prosecutor's Offices and investigative units (such as the S.C.O. of the State Police and the R.O.S. of the Carabinieri) systematically resort to latest-generation technological tools. Criminal enforcement relies on **covert cyber-wiretapping via software implants (trojan horses)** deployed into traffickers' devices. Big Data analytics and blockchain forensics enable the mapping of illicit financial transactions destined for paying travel debts and laundering money, disarticulating the national branches of complex transnational cartels.
- **The New Trends and the European Framework**: As highlighted by the **Fifth Report of the European Commission**, the criminal networks operating in Italy have digitized. The predominant method of recruitment for sexual exploitation is the "**lover boy**" model, where traffickers target victims online via social media and, by simulating romantic relationships, convince them to move to Italy from third countries only to force them into forced prostitution. The Report also highlights high-tech hybrid organizational models, such as Chinese criminal networks. The latter manage sexual exploitation through **decentralized call centers** located between China and the EU, which operate as digital hubs to

schedule online advertising on classified sites, fix rates and appointments, and launder illicit proceeds through secure digital transactions.

**FOCUS**

**The "Madams" System**

On the criminal scene, a new organizational model has emerged, falling under the scope of foreign mafia-type associations pursuant to **Art. 416-*bis* of the Criminal Code**, which is entirely female-driven: a mafia that can be defined as "gender-based", given that leadership and control positions are held by women, the so-called "**madams**", whose victims are exclusively young women from their same country. These female bosses lead an apparent low-profile life in destination countries (like Italy) and, once they return to their homeland in Nigeria, they invest the proceeds from the sexual exploitation of their victims in real estate or legal businesses.

The organization's scheme is based on a complex **geographical and digital triangulation**:

1. The first command center is headed by the local madam located in Nigeria (e.g., in Benin City), who recruits vulnerable girls from poor families, binding them psychologically and spiritually through subjugation rituals (e.g., *juju* rituals).
2. The transit outpost is managed by a second madam in Libya, who cooperates with local militias and armed groups, paying duties and managing via smartphones the migratory transit of the victims across the Mediterranean.
3. The reception center is presided over by the madam stationed in the destination country (Italy), who takes charge of the girls, confiscates their documents, assigns them an exorbitant extortionate debt (up to 50,000 euros), and forces them into the street or indoor prostitution circuit. Serving the madam are exclusively men for executive tasks and violent territorial control (the so-called trolley men), responsible for physically and electronically monitoring the girls' movements. The criminal association thus commits multiple transnational crimes: from human trafficking to international money laundering.

## X. What Legal Pathways Define the Criminalization of Trafficking Under Domestic Law?

Following recent evolutions in migratory flows, Italy must be considered a country heavily impacted by the crime of trafficking. There is a continuous increase in individuals who, to afford their journey, rely on criminal organizations that bind them to situations of exploitation, both in transit and destination countries. Early identification of victims is essential to ensure their protection and assistance. First and foremost, Law Enforcement Agencies, through Operational Departments and specialized Units, collaborate with local entities and associations to identify situations of exploitation.

Equally important are the **Territorial Commissions for the Recognition of International Protection**, which, during the examination of asylum applications, are trained to recognize indicators of trafficking (e.g., narrative inconsistencies, unusual travel debts, psychological subjection) and initiate the referral (transfer) process toward competent services. Within the framework of the project "Coordination Mechanisms for Victims of Trafficking," promoted by UNHCR and the National Commission for the Right to Asylum (CNDA), Standard Operating Procedures (SOPs) for the identification

and referral of victims have also been defined, with particular attention to women and children.

In the Italian legal system, **Art. 18 of Legislative Decree 286/1998 (Consolidated Law on Immigration)**, as amended by Legislative Decree No. 24/2014, provides for a victim protection program with annexed legal and psychological assistance, as well as support for social integration. More precisely, it defines projects implemented at the local level aimed at ensuring adequate assistance measures – initially provided on a transitional basis and subsequently aimed at final social inclusion – for individuals found in conditions of severe exploitation due to crimes of reduction to or maintenance in slavery and trafficking in persons. The interventions and services of anti-trafficking entities are divided into: contact, detection, identification, and protection actions for the individual; listening desks, shelter intake, including secure safe houses with secret addresses; accompaniment toward socio-labor inclusion; and socio-legal assistance.

- **The Integration of Digital Tools**: Beyond traditional street units, national entities and NGOs adopt secure digital channels to foster the detection of victims. They develop **multilingual web help platforms and secure geolocation apps**, allowing individuals in states of forced isolation or indoor confinement to send traceable requests for help. This data is then securely managed by the National Anti-Trafficking Hotline, ensuring anonymity and the real-time activation of protection procedures on the ground.

**FOCUS**

**National Referral Mechanism for the Identification, Assistance and Protection of Victims of Human Trafficking and/or Severe Exploitation, 2023**

In coherence with the national strategy outlined by the National Anti-Trafficking Action Plan 2022-2025 (PNA), this constitutes the instrument through which the State fulfills its obligations to protect and promote the human rights of trafficking victims, enabling the correct and early identification of victims and their assistance. The National Referral Mechanism materializes as a set of recommendations and practical measures that include a detailed series of **Standard Operating Procedures (SOPs)**. These consist of distinct measures designed to facilitate secure interaction among judicial authorities, labor inspectorates, healthcare facilities, and assistance associations, ensuring early intake and preventing the secondary victimization of the vulnerable individual throughout the entire bureaucratic and jurisdictional process.

## XI. Key Findings

- **Human trafficking is a growing transnational crime**: It represents the most significant expression of "borderless" illicit activity conducted by transnational criminal syndicates. In addition to being an abhorrent violation of human rights, it constitutes a genuine global public safety issue. The most recent trends, confirmed by the **Fifth Report of the European Commission**, highlight the structuring of flexible networks capable of leveraging digital vectors, as demonstrated by the management of transnational call centers aimed at online advertising and the centralized monetization of proceeds derived from trafficking.
- **The prevalent form of trafficking is the sexual exploitation of women and minors**: Modalities vary based on geographical, socio-economic, and cultural factors. Globally, women and girls account for approximately **72% of trafficking**

**victims**, with a rising incidence among minors. The most affected regions include sub-Saharan Africa, South Asia, and Central America and the Caribbean, where the minor component often exceeds 50% of cases, highlighting a stark gender asymmetry that predominantly earmarks the female population for prostitution and bodily commodification.

- **Smuggling of migrants and trafficking in persons - Frequently blurred boundaries**: This is due to numerous practical overlaps and shared criminal dynamics. Although distinct from a legal standpoint (with smuggling being a crime against the State and trafficking being a crime against the person), in daily reality, these phenomena frequently intertwine. Irregular migration routes systematically convert into trafficking contexts as soon as smugglers abuse the irregular status or debts contracted by migrants, reducing them to a state of continuous subjection.
- **A vigorous and stringent international, European, and national regulatory response**: The international community has developed a robust and integrated regulatory framework to counter human trafficking, particularly for the purpose of sexual exploitation, through a combination of policies and collaborations with public, private, and international organizations. This framework, coordinated at the European level via Art. 83 of the TFEU and the recent **Directive (EU) 2024/1712**, finds full alignment in Italy through the rigorous application of Art. 600 and Art. 601 of the Criminal Code integrated with social protection pursuant to Art. 18 of the Consolidated Law on Immigration.
- **The use of digital technologies has transformed the landscape of human trafficking**: The use of digital technologies has radically transformed the crime of human trafficking, introducing new modalities for recruiting, exploiting, and controlling victims. Traffickers employ *e-hunting* on social networks, the *lover boy* method in a virtual key, and artificial intelligence tools for the production of blackmailing *deepfakes*. This phenomenon constitutes a growing challenge for authorities and organizations engaged in the fight against trafficking, demanding the adoption of advanced cyber-forensic methodologies and OSINT (Open Source Intelligence) investigations.
- **Italy and anti-trafficking mechanisms**: The National Anti-Trafficking Action Plan, updated for the 2022-2025 period, represents the central strategy of the Italian government for the prevention, identification, and protection of trafficking victims. Based on the inter-institutional integration of the National Referral Mechanism (NRM), the national system operates effectively at the local level as well, where numerous Prefectures, Prosecutor's Offices, and Regions have signed territorial memoranda of understanding to consolidate the protection network and intake in safe houses at secret addresses, while simultaneously dismantling complex mafia models such as Nigerian female-led criminal organizations (*madams*).

# Illicit Drug Trafficking

*by Emanuela Coppola and Fernanda Masullo*[*]

SUMMARY: I. What is the Geopolitical and Dogmatic Framework of Global Drug Trafficking? – II. How is the Scheduling System Organized Under the United Nations Conventions? – III. What Treaty Instruments has the International Community Established against Precursor Diversion? – IV. What Monitoring standards has the Council of Europe adopted through the Pompidou Group? – V. How does the European Union Exercise its Shared Criminal Competence Regarding Narcotics? – VI. How is the Eurounitarian Harmonization of Drug Offenses and Sanctions Structured? – VII. How have International and European Drug Trafficking Sources been Transposed into Domestic Law? – VIII. What are the Main Judicial Criteria for Distinguishing Minor Dealing from Structured Trafficking? – IX. What is the Logistical Impact of New Information Technologies and Crypto-Markets on Trafficking? – X. What is the Logistical Impact of New Information Technologies and Crypto-Markets on Trafficking?

KEY FINDINGS: Configuration of drug trafficking as a Eurocrime; Integration and timely contrast of New Psychoactive Substances (NPS); Reliance on special investigative techniques and JITs; Transition towards Hyper-Digitalization and the Common Operational Space; Structural severity of the Italian legal system.

## I. What is the Geopolitical and Dogmatic Framework of Global Drug Trafficking?

Illicit trafficking in narcotic drugs and psychotropic substances represents, from a geopolitical, historical, and criminological perspective, the most lucrative, flexible, and extensive illegal market on the planet. It constitutes the genetic core around which the modern structures of transnational organized crime have evolved. It is not a circumscribed criminal violation that can be tackled through isolated domestic policies, but rather an asymmetric, subversive phenomenon that requires a coordinated approach starting from the global level. Modern drug cartels operate as true economic multinationals equipped with massive financial resources, logistical networks that cross continents, and capillary distribution channels.

Drug trafficking constitutes a threat of global interest to international stability and security, acting through three highly destructive vectors that we must remember:

- **Terrorist Financing and Narco-terrorism**: There is an established structural and financial link between the proceeds of drug trafficking and the funding of terrorist cells or subversive paramilitary groups, which utilize control over plantations and transit routes to self-finance and purchase weaponry.

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

- **Corruption and Infiltration of State Apparatuses**: The immense flows of illicit capital generated by large-scale trafficking are used to corrupt public officials, influence democratic processes in developing countries, and pollute legal economic markets in advanced nations through sophisticated and pervasive money laundering operations.
- **Violation of Public Health and Safety**: The proliferation of traditional narcotics and the emergence of high-lethality synthetic drugs erode the social fabric, overburden national healthcare systems, and violate the core rights to life and security of the person protected by the European Convention on Human Rights (ECHR)

**FOCUS**

**The Hyper-Digitalization of Global Drug Trafficking**

In the current geopolitical scenario, global drug trafficking networks have undergone a radical technological mutation resulting from the digital transition. International cartels no longer depend exclusively on traditional physical drug dealing squares or street-level smuggling but have implemented a cybernetic and asymmetric operational model for global distribution. Among the profiles of greatest social alarm monitored by the UN are:

- The exploitation of clandestine marketplaces located within the Darknet (the so-called Crypto-Markets), where the wholesale and retail purchase and sale of narcotics occur in total anonymity.
- The systematic use of decentralized cryptocurrencies characterized by high levels of anonymity (privacy coins like Monero) and financial mixing services (crypto-mixers) to conceal the origin of illicit financial flows, evading the monitoring of Financial Intelligence Units.
- The reliance on end-to-end encrypted messaging systems equipped with self-destruct timers to coordinate the logistics of containers and maritime landings without leaving forensic traces usable by investigators.
- The employment of ordinary postal shipping channels and international express couriers split into thousands of illicit micro-loads, a technique termed micro-trafficking designed to make mass customs checks statistically impossible.

## II. How is the Scheduling System Organized under the United Nations Conventions?

The housing of the global legal response is built on overcoming the fragmentation of laws among individual States by creating a universal and uniform control system coordinated by the United Nations. Dogmatically, the definition of the drug trafficking offense at the global level is not enclosed within a single legislative text but is structured across three fundamental UN Conventions that form the backbone of international criminal law on the matter:

- The Single Convention on Narcotic Drugs (New York, 1961): As amended by the 1972 Protocol, it unified previous fragmented treaties, establishing a global system for controlling and limiting plant-based substances of natural origin (opium, cannabis, coca), strictly prohibiting their production and trade for purposes other than those strictly medical and scientific.
- The Convention on Psychotropic Substances (Vienna, 1971): Designed to respond to the social alarm generated by the mass proliferation of laboratory-made chemical substances (hallucinogens, amphetamines, barbiturates, tranquilizers),

placing them within specific international control schedules differentiated by intrinsic danger and potential therapeutic value.

- The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna, 1988): Represents the true global enforcement and judicial pillar, focused on the international criminalization of the illicit commercial supply chain, introducing for the first time the mandatory obligation to combat money laundering and incentivizing special investigative techniques.

**REFERENCES**

**United Nations Vienna Convention against Illicit Traffic, 1988, Art. 3**

"Each Party shall adopt such measures as may be necessary to establish as criminal offences under its domestic law production, manufacture, extraction, preparation, offering, offering for sale, distribution, sale, delivery on any terms whatsoever, brokerage, dispatch, dispatch in transit, transport, importation or exportation of any narcotic drug or psychotropic substance contrary to the provisions of the 1961 Convention or the 1971 Convention, as well as the organization, management or financing of these illicit operations, when committed intentionally."

**United Nations Vienna Convention against Illicit Traffic, 1988, Art. 12**

"This provision establishes a strict and innovative international surveillance regime over the legitimate trade of base chemical substances (precursors or essential chemicals) frequently diverted by traffickers for drug synthesis. It imposes an obligation on States to monitor the manufacture, as well as the domestic and foreign distribution of these substances, to establish a licensing system for customs import and export, and to promptly notify the INCB of any commercial transaction or shipment that presents profiles of anomaly or suspicion."

To facilitate memorization, the constituent elements of the global enforcement action set by the UN that we must remember are:

- **The Principle of Strict Statutory Scheduling**: No substance or molecule can be criminally prosecuted or seized on an international scale unless it is formally included and classified within the four attached Schedules to the UN treaties, which are constantly updated by supranational scientific bodies.
- **The Distinction between Trafficking and Personal Consumption**: While the Conventions mandate severe, liberty-depriving criminal repression for the commercial activities of drug trafficking, Art. 3 of the 1988 Convention leaves Member States a margin of discretion in punishing mere possession or purchase for personal consumption, allowing – in accordance with domestic constitutional principles – alternative measures to imprisonment, such as treatment, education, and social rehabilitation.
- **The Role of New Technologies and the Challenge of Molecular Automation** (Integration): The UN's principle of strict statutory scheduling currently faces a structural crisis caused by new chemical-information technologies. Criminal cartels utilize predictive Artificial Intelligence software and automated synthesis to modify the molecular structure of existing substances, creating New Psychoactive Substances (NPS) in laboratories before UN bodies can map their illegality. This phenomenon of chemical hacking temporarily eludes the traditional incrimination parameters of the 1961 and 1971 Conventions. Conversely, the World Health Organization (WHO) and the INCB utilize advanced algorithms and Big Data Analysis systems to intercept emerging

molecules early on the web and fast-track urgent inclusion procedures into international schedules.

- **Italian Domestic Law Profiles and the National Scheduling System** (Integration): The internal criminal legal system transposes and declines this multi-level international framework through Presidential Decree No. 309 of October 9, 1990 (Consolidated Law on Narcotic Drugs). The Italian legislator respects the principle of legality by structuring the incrimination system of Art. 73 and Art. 74 of P.D. 309/90 on the basis of five attached domestic ministerial schedules, constantly updated by the Ministry of Health. This mechanism ensures compliance with the principles of specificity and determinacy, sharply distinguishing conducts based on the type of drug (hard or soft) and whether the purpose of criminal behavior is commercial trafficking or personal consumption.

**FOCUS**

**The Multi-Level Regulatory Structure of the Drug Trafficking Offense**

- **International level** (UN): Vienna Conventions (1961, 1971, 1988). Focus centered on global substance schedules and universal criminal obligations to incriminate the commercial supply chain. Operational tools include extradition mandates and assisted confiscation of illicit capital.
- **Regional level** (Council of Europe): Pompidou Group (established in 1971). Focus directed toward monitoring new flows and public health prevention. Provides multidisciplinary control platforms and guarantees compliance with the human rights parameters of the ECHR.
- **European Union level** (EU): Council Framework Decision 2004/757/JHA and the new EUDA Agency. Focus on the harmonization of minimum criminal sanctions within the single market to prevent forum shopping. Application tools activate the European Arrest Warrant and the EMPACT operational network.
- **National level** (Italy): Italian Criminal Legal System (P.D. 309/1990). Focus anchored on the domestic scheduling system (Art. 73 and Art. 74). Provides prosecutors with the tools for a clear distinction between personal use and structured dealing.

## III. What Treaty Instruments has the International Community Established Against Precursor Diversion?

The functioning and stability of the global sanctioning system rest upon a complex and permanent institutional architecture established within the United Nations, whose primary task is to monitor the exact execution of obligations contracted by the signatory States. We must understand that global enforcement does not focus solely on the final drug product but requires rigorous oversight over the legitimate commercial chemical industry. The executive and monitoring apparatus of the UN is structured around two central control bodies:

- **The United Nations Office on Drugs and Crime** (UNODC): Headquartered in Vienna, it constitutes the strategic and operational coordination body that analyzes global trends in illicit markets, publishing the World Drug Report annually. The UNODC provides technical and financial assistance to Member States in aligning their domestic criminal legislation, implementing customs intelligence techniques, and dismantling global supply routes.
- **The International Narcotics Control Board** (INCB): An independent and quasi-judicial body of experts established by the 1961 Convention. The INCB holds the

critical competence of estimating the legitimate global requirement (medical and pharmaceutical) of opiates and psychotropic substances, exercising stringent surveillance to prevent the phenomenon of precursor chemical diversion from legal industries to clandestine laboratories controlled by mafia cartels.

**FOCUS**

**Global Initiatives against the Synthetic Opioid Crisis**

The most recent reports and global alerts issued by the UNODC highlight that the most lethal threat to international security is currently represented by the exponential explosion of the illicit market for synthetic narcotics, with specific reference to Fentanyl and its chemical analogues (synthetic opioids up to one hundred times more potent than morphine). Since these are entirely chemical molecules, cartels do not need control over agricultural lands (plantations) but establish mobile urban laboratories by illegally importing dual-use precursor chemicals from third countries. To curb this phenomenon, the international community has promoted the Global Coalition to Address Synthetic Drug Threats, aimed at fostering an instantaneous exchange of toxicological data and developing common forensic protocols to intercept emerging chemical precursors before they are formally scheduled.

## IV. What Monitoring Standards has the Council of Europe Adopted through the Pompidou Group?

In transitioning from the universal to the European regional level, the Council of Europe addresses the threat of drug trafficking through an approach that bridges the rigor of criminal sanctions with the protection of public health, harm reduction, and the safeguarding of human rights. The cornerstone institutional tool of the Council is the international cooperation group on drugs and addictions, historically known as the **Pompidou Group**, established in 1971 and formally integrated into the framework of the Council of Europe in 1980. The three operational pillars of the Pompidou Group are:

1. **Judicial and Operational Cooperation**: Strengthening the immediate exchange of operational data and information between magistrates and law enforcement investigators to intercept trafficking vectors across cross-border road, airport, and maritime networks.
2. **Public Health Standards**: Developing uniform scientific guidelines and models for prevention, therapeutic treatment of addictions, and the implementation of rehabilitation programs within European prison systems.
3. **Guarantee of Human Rights**: Constant vigilance to ensure that the application of emergency anti-mafia and anti-drug regulations does not disproportionately compress the fundamental rights of defense (Art. 6 ECHR) or the principle of legality and proportionality of sentences (Art. 7 ECHR).

Within the framework of this multi-level strategy, the Council of Europe adopted the pivotal “Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime” (Strasbourg, 1990). This treaty applies with absolute priority to the capital accumulated by drug trafficking cartels, providing Member States with an advanced technical tool for cross-border asset aggression, bypassing the need to stipulate complex bilateral agreements and directly striking the economic core of illicit drug trafficking.

## V. How does the European Union Exercise its Shared Criminal Competence Regarding Narcotics?

The European Union considers the international trafficking of narcotics a direct threat to the stability of the single market and the security of the common area. Consequently, the Treaty of Lisbon formally included illicit drug trafficking within the exhaustive list of Eurocrimes, granting European institutions the legitimacy to intervene through the instrument of minimum rules to approximate national criminal codes and counter the phenomenon on common grounds.
The core legal basis that we must remember is Art. 83, Para. 1 of the Treaty on the Functioning of the European Union (TFEU), which vests the Parliament and the Council with the competence to establish directives aimed at harmonizing the definitions of offenses and the scale of applicable sanctions in spheres of particularly serious crime characterized by a clear and intrinsic transnational dimension.

**REFERENCES**

**Treaty on the Functioning of the European Union, Art. 83 para. 1**
"The European Parliament and the Council, acting by means of directives in accordance with the ordinary legislative procedure, may establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism, trafficking in human beings (...), illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime."

The institutional and security architecture of the European Union has taken a fundamental step forward with the entry into force of the operational mandate of the new European Union Drugs Agency (EUDA), established by Regulation (EU) 2023/1322 to replace the old and limited European Monitoring Center (EMCDDA).
The establishment of the EUDA responds to the Union's strategic need to equip itself with a proactive security and early warning body, moving past the old model based on mere passive statistical collection. The new agency exercises incisive powers structured along three core pillars:

- Early Warning System (EWS): Continuous monitoring of digital networks and immediate chemical identification of New Psychoactive Substances (NPS) to arrange for their simultaneous criminal ban across the entire Union.
- Security Threat Assessment: Developing forensic analysis, predictive models, and technical investigations into the logistics of large international cartels and their infiltration into major European logistical and port hubs (such as the ports of Antwerp and Rotterdam).
- National Capacity Building: Direct technical, scientific, and financial assistance to the toxicological and forensic laboratories of Member States' law enforcement agencies, standardizing their capabilities to detect synthetic drugs and emerging chemical precursors.

## VI. How is the Eurounitarian Harmonization of Drug Offenses and Sanctions Structured?

The regulatory pillar of criminal harmonization regarding narcotics within the Area of Freedom, Security and Justice is constituted by Council Framework Decision 2004/757/JHA, subsequently amended and strengthened by Directive (EU) 2017/2103. This instrument defines the minimum behaviors linked to drug trafficking that all Member States are obliged to punish with effective, proportionate, and dissuasive sanctions, preventing traffickers from exploiting loopholes or disparities in legal treatment among different countries of the Union to practice so-called forum shopping.
The EU discipline expressly excludes from the scope of mandatory harmonization those conducts connected to mere personal drug consumption, the regulation and criminal or administrative classification of which remains entrusted to the full sovereignty and autonomy of individual Member States.

**REFERENCES**

**Council Framework Decision 757/JHA, 2004, Art. 2, Art. 3 and Art. 4**
The regulation establishes that each Member State adopts the necessary measures to ensure that intentional offenses of cultivation, production, manufacture, offering, sale, distribution, transport, import, and export of drugs and precursors are punishable. Art. 4 imposes a mandatory obligation to provide for maximum statutory penalties of no less than a duration between 5 and 10 years of imprisonment if the act is of significant gravity, involves large quantities of highly toxic substances, or is committed within the framework of a criminal organization pursuant to Framework Decision 2008/841/JHA

The reform introduced by Directive (EU) 2017/2103 accelerated the enforcement against synthetic molecules placed on the market by clandestine chemical laboratories to circumvent the law:

- **Interception**: The new synthetic substance is intercepted on the market or on the web and immediately reported to the EUDA's Early Warning System.
- **Scientific Evaluation**: The EUDA agency compiles an urgent scientific report in a very short timeframe, analyzing its toxicity index and the potential rate of abuse for public health.
- **Automatic European Inclusion**: The European Commission, through delegated acts, directly inserts the molecule into the definition of "drug" annexed to Framework Decision 2004/757/JHA. This mechanism concept obliges all Member States to punish its manufacture and dealing within the same minimum statutory terms, neutralizing the lengthy delays of domestic parliamentary debates and decrees.

**CASE STUDY**

**Court of Justice of the European Union, B.S. and C.A., 2020**

An essential jurisprudential point of reference is the famous judgment of the Court of Justice of the European Union regarding the free movement of goods and the definition of a narcotic drug. The CJEU was called upon to determine whether cannabidiol (CBD) extracted entirely from the cannabis sativa plant could be classified as a "drug" within the meaning of Framework Decision 2004/757/JHA and the UN Conventions. The Court ruled that, based on available scientific knowledge, CBD does not present psychotropic or harmful effects on human health, unlike THC. Consequently, the Court held that it does not fall within the criminal definition of a drug, declaring unlawful the national commercial bans applied in the absence of a real and proven health risk, thereby confirming the primacy of EU law and scientific evidence over the restrictive interpretations of individual national legislators.

## VII. How have International and European Drug Trafficking Sources been Transposed into Domestic Law?

The Italian legal system possesses one of the most stringent and detailed criminal and preventive legislations on narcotics, heavily influenced by historical national experience in countering mafia-type criminal syndicates. The core regulatory source governing the entire matter is **Presidential Decree No. 309 of October 9, 1990** (Consolidated Law on Narcotic Drugs), amended multiple times to adapt it to the obligations arising from the 1988 Vienna Convention and European directives.

The repressive architecture of the Consolidated Law rests on the binary combination of two fundamental articles:

- **Art. 73 of P.D. 309/1990 (Illicit production, trafficking, and possession)**: Punishes the conducts of cultivation, production, manufacture, extraction, possession, offering, putting on sale, and illicit trade of substances listed in the ministerial schedules. The penalty varies significantly depending on the nature of the substance: for "hard drugs" (*droghe pesanti* - schedules I and III, e.g., cocaine, heroin), the penalty is imprisonment from 6 to 20 years and a fine; for "soft drugs" (*droghe leggere* - schedules II and IV, e.g., cannabis), imprisonment ranges from 2 to 6 years. Para. 5 regulates the autonomous mitigated circumstance for offenses deemed of minor entity (*lieve entità*).
- **Art. 74 of P.D. 309/1990 (Association aimed at illicit trafficking)**: Configures an autonomous and extremely serious special associative crime (an offense involving collective conduct). It punishes with imprisonment of no less than twenty years anyone who promotes, establishes, directs, organizes, or finances a syndicate composed of three or more persons aimed at committing the offenses referred to in Art. 73, elevating the penalty for participants and providing for severe aggravating circumstances if the association is armed.

**REFERENCES**

**Italian P.D. 309, 1990, Art. 8**

The penalty for the offenses referred to in Art. 73 is increased by one-third to one-half when the substances are delivered or destined to minors, when the act is committed by three or more persons in conspiracy, or when the substances are adulterated or mixed in such a way as to increase their toxicity or danger. If the act assumes a transnational character, the common special-effect aggravating circumstance pursuant to Art. 61-*bis* of the Criminal Code also applies (introduced into the system through the transposition of Law 146/2006).

## VIII. What are the Main Judicial Criteria for Distinguishing Minor Dealing from Structured Trafficking?

In the Italian criminal system, the boundaries between the administrative relevance of personal consumption (Art. 75 of P.D. 309/1990) and the criminalization of ordinary street dealing or large-scale cargo trafficking have been the subject of constant and evolving jurisprudential refinement, aimed at ensuring compliance with the constitutional principles of offensiveness, proportionality of sanctions, and criminal strictness (*tassatività penale*).

**CASE STUDY**

**Italian Cassation Court, Joint Sections, Judgment No. 35222, 2023**

The Joint Sections of the Supreme Court of Cassation intervened to resolve a crucial interpretative conflict regarding the relationship and coexistence between common criminal conspiracy (Art. 416 of the Criminal Code), mafia-type association (Art. 416-*bis* of the Criminal Code), and association aimed at narcotics trafficking (Art. 74 of P.D. 309/1990). The judges of legitimacy ruled that the formal concurrence between the crime of mafia association and that of drug trafficking is fully configurable whenever the mafia clan uses its intimidation power and hegemonic control over territory to monopolize or protect the management of drug dealing squares (*piazze di spaccio*), while simultaneously operating as an autonomous structure aimed at international drug trafficking.

Parallel to this, the jurisprudence of legitimacy has consolidated extremely rigid criteria for the application of the minor entity clause under Art. 73, Para. 5, establishing that the mildness of the act can only be recognized if the conduct, assessed comprehensively based on the means used, the modalities of action, the occasional disposition of the offender, and the quality/quantity of the seized substances, displays reduced offensiveness, strictly excluding the benefit in the presence of stable supply channels or links to networks of transnational significance.

## IX. What is the Logistical Impact of New Information Technologies and Crypto-Markets on Trafficking?

Modern drug trafficking has undergone a profound process of hyper-digitalization, partially decoupling itself from traditional physical distribution networks. Criminal cartels utilize cyberspace to manage logistics, sales, and the subsequent laundering of dirty money, posing complex challenges to the digital forensics units of law enforcement agencies. Conversely, judicial police officers operate under exceptional procedural

derogations pursuant to **Art. 9 of Law 146/2006** and with the strategic support of agencies within the Area of Freedom, Security and Justice. The special anti-drug investigative techniques based on Law 146/2006 are:

- Undercover Operations: Judicial police officers from the Central Directorate for Anti-Drug Services (DCSA) can infiltrate logistical or digital networks, simulating the purchase of drug shipments or providing fictitious logistical services to the gangs. This conduct is protected by a special cause of exclusion of punishability in order to gather stable evidence from within the criminal structure.
- Controlled Deliveries: This allows magistrates to order the deferral or delaying of the seizure (delayed seizure) of narcotics intercepted at frontiers, ports, or airports. The cargo is monitored during its road or maritime transit to identify the real recipients, directors, and top-tier promoters of the drug trafficking network.

**FOCUS**

**The Dismantling of Crypto-Markets**

Retail and wholesale distribution has relocated within illegal marketplaces hosted on the Dark Web (crypto-markets accessible via TOR networks). Traffickers utilize modified smartphones with encrypted communication operating systems (such as Sky ECC or EncroChat) and payments in fortified cryptocurrencies (Monero), shielded by mixing services. European agencies (Europol and Eurojust) have reacted with coordinated global operations (e.g., Operation Desert Light), decrypting secure servers and establishing Joint Investigation Teams (JITs) to simultaneously arrest cartel leadership stationed in offshore hubs like Dubai and execute preventive asset seizures in real time.

## X. How do Specialized European Agencies Coordinate Asset Aggression against International Cartels?

The fight against international narcotics trafficking cannot be separated from a systematic strategy of asset aggression. Depriving cartels of their immense capital flows constitutes the only effective tool to neutralize the operational capacity of criminal networks and prevent the reinvestment of illicit proceeds into the legal economy.

Within the European Union, this strategic coordination is driven by the *follow the money* principle and leverages the interoperability of specialized agencies within the Area of Freedom, Security and Justice:

- **Europol**: Through the **European Financial and Economic Crime Centre (EFECC)**, it supports Member States in tracking illicit financial flows. Europol cross-references data derived from decrypted communication platforms (such as EncroChat and Sky ECC) with suspicious transaction reports, identifying cryptocurrency transactions and international money laundering channels.
- **Eurojust**: It plays a crucial role in the judicial phase, coordinating the simultaneous execution of cross-border asset seizure and freezing orders. Through the network of **Asset Recovery Offices (AROs)** and close cooperation with the European Public Prosecutor's Office (EPPO), Eurojust ensures the application of the principle of mutual recognition to asset-blocking measures, preventing traffickers from shifting capital to more lenient offshore jurisdictions.

**FOCUS**

**The Dismantling of the "Super Cartel" (Operation Desert Light)**

A capstone example of coordinated operational practice between agencies is the international operation "Desert Light," led by Europol and Eurojust. The investigation targeted a "super cartel" that controlled over one-third of the total cocaine trafficking into the European Union, operating simultaneously from logistical hubs located in Dubai, the Netherlands, Belgium, Spain, and France. Thanks to the decryption of the messaging platforms utilized by the criminals, investigators were able to cross-reference criminal intelligence flows. Coordinated by Eurojust, magistrates from different nations simultaneously issued European Arrest Warrants and European Investigation Orders, leading to coordinated arrests in Europe and the United Arab Emirates, alongside the preventive seizure of assets and movable property worth hundreds of millions of euros, demonstrating the effectiveness of the intelligence-led policing model.

The European Enforcement Architecture against Drug Trafficking (ports and sanitary border) is made up of:

- **Information Hub (Europol - ECTC)**: Centralization of cryptographic data decoded from seized chats and tracking of international money laundering flows managed within tax havens.
- **Judicial Hub (Eurojust)**: Immediate resolution of positive or negative conflicts of jurisdiction and establishment of Joint Investigation Teams (JITs) to allow the cross-border use of evidence without traditional letters rogatory.
- **Operational Hub (EMPACT 2026-2029)**: Field execution of coordinated Action Days, arranging mass customs checks and technological investigations within the main maritime port hubs of the European Union.

## XI. Key Findings

The scientific and regulatory analysis carried out within this paper leads to the delineation of five fundamental findings that we must assimilate for the purpose of understanding the subject matter.

Configuration of drug trafficking as a Eurocrime: Pursuant to Art. 83, Para. 1 of the TFEU, illicit drug trafficking is codified as a sphere of particularly serious crime characterized by a marked cross-border dimension, legitimizing the European Union to establish common minimum definitions and sanctions within the unified legal space to prevent the phenomenon of forum shopping.

- **Integration and timely contrast of New Psychoactive Substances (NPS)**: The evolution of the European regulatory framework (the reform under Directive (EU) 2017/2103 which amended Council Framework Decision 2004/757/JHA) extended the notion of a narcotic drug to next-generation synthetic molecules (such as fentanyl and its chemical analogues), ensuring uniform criminal prosecution as soon as they are intercepted by the Early Warning System of the new European Union Drugs Agency (EUDA).
- **Structural severity of the Italian legal system:** The Italian domestic penal system stands out for a double-track sanzionatory framework contained in Presidential Decree 309/1990, centered on the sharp distinction between the offense of ordinary trafficking (Art. 73) and the autonomous offense of association aimed at drug trafficking (Art. 74, punished with a minimum penalty

of no less than twenty years), coordinated with the transnational aggravating circumstance pursuant to Art. 61-*bis* of the Criminal Code (introduced by Law 146/2006).

- **Reliance on special investigative techniques and JITs**: The fight against international cartels demands the proactive and coordinated deployment of undercover operations and controlled deliveries pursuant to Art. 9 of Law 146/2006. The admissibility and stability of evidence gathered across borders depend on the establishment of Joint Investigation Teams (JITs) managed by Eurojust, which eliminate the cumbersome procedures of traditional letters rogatory.
- **Transition towards Hyper-Digitalization and the Common Operational Space**: Modern illicit markets develop within the Dark Web and utilize cryptocurrency payments, requiring advanced digital forensics capabilities. The European Union's institutional response focuses on the model of intelligence-led policing coordinated by specialized agencies (Europol, Eurojust), striking central high-risk networks and arranging the immediate freezing of criminal assets accumulated within offshore financial channels (Operation Desert Light).

# 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.

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.

# Corruption

*by Christian Fausto Santoriello*[*]

SUMMARY: I. How Do Fraud and Corruption Cases Influence Trust in Public Institutions? – II. Which Provisions Allow the European Union to Protect Its Financial Interests? – III. How Does the PIF Directive Define Active and Passive Corruption? – IV. What Jurisdictional Conflicts Exist Between PIF Crimes and National Jurisdictions? – V. How Does the International Definition of Corruption Differ from the European One? – VI. What Substantive Sanctioning Instruments Define the Offense of Corruption Under Domestic Law? – VII. What Legislative Phases Produced the European Regulations Currently in Force Regarding Enforcement? – VIII. Which Historical Cases Marked the Institutional Evolution from UCLAF To OLAF? – IX. How Do Specialized European Agencies Practically Operate in Combating Public Corruption? – X. What Geopolitical Implications Do Corruption and Illicit Lobbying Entail for Transparency Policies? – XI. How Do "Better Regulation" Strategies Connect with The Digitalization of Anti-Corruption Processes?

KEY FINDINGS: Budget protection as a subsidiary Eurocrime; Dogmatic classification of conducts and VAT fraud; Severity and anticipation of protection in the Italian legal system; Institutional evolution driven by real-world crises; The operational tandem and the limits of EPPO, Eurojust, and Europol.

## I. How Do Fraud and Corruption Cases Influence Trust in Public Institutions?

Corruption and fraud against public resources do not constitute mere offenses of an economic-financial nature; rather, they represent a severe **asymmetric threat to democratic stability** and the social cohesion of multilevel legal systems. According to consolidated sociological-legal studies, continental public opinion manifests deep scepticism regarding the effectiveness and actual incisiveness of the instruments established by States to repress and punish these eversive phenomena.
This systemic pathology poisons the bond of trust between citizens and institutions, acting on three specific system axes that must be remembered:

- **Erosion of Institutional Credibility:** Over two-thirds of European citizens believe that the phenomenon of corruption is not effectively countered, negatively affecting the perceived reliability of the bureaucratic and administrative apparatus, primarily at the national level and, consequently, at the Euro-unitarian level.

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

ISSN: 2717-1914 / 

- **Distrust in Political Governance:** More than half of the Union's population accuses its governments of structural incapacity in containing illicit behaviors and conflicts of interest.
- **Social Normalization of Malfeasance:** In territorial areas with a high density of organized crime, the submission of citizens to extortionate or corrupt practices (granting money or undue favors in exchange for services that constitute perfect subjective rights) is embedded within a retrograde mindset. This distortion leads to systemic illegality being perceived as an ordinary and inevitable practice of the public machine.

From a dogmatic and statistical perspective, the level of dissemination of the phenomenon within individual States can be analyzed through a specific global macroeconomic indicator, called the **Corruption Perception Index (CPI)**, developed annually by Transparency International.

**FOCUS**

**The Corruption Perception Index and the Checks Model**

The CPI Index examines 180 countries worldwide, assigning to each a conventional score between **0 (highest level of perceived corruption)** and **100 (ideally incorrupt State)**. The qualitative analysis of the data reveals the following global stratification:

**The Scandinavian Model (Top of the rankings):** No State is immune to risk, but Denmark ranks stably at the global peak with a score of **90/100**, followed by Finland, Singapore, New Zealand, Luxembourg, and Norway. This data highlights how Nordic countries possess bureaucratic structures characterized by high levels of transparency, administrative solidity, and rigorous ethical codes. These factors enable the correct constitutional functioning of a system of **"checks and balances" (controls and counterweights)**, wherein the clear separation of functions and the interoperability of cross-checks make it technically complex to carry out abuses of office or misappropriation of funds without immediate detection by a third, independent supervisory body.

**High-Risk Systems (Bottom of the rankings):** The final positions are occupied by developing countries or those destabilized by humanitarian crises, famines, and internal armed conflicts (such as South Sudan, Somalia, Venezuela, Syria, Yemen, and Libya). In these contexts, mass poverty, political instability, and the absence of independent oversight authorities operate as intrinsic factors that create fertile ground for the proliferation of fraudulent conduct and the embezzlement of international aid.

**The Position of Italy:** The Italian legal system suffers from historical structural weaknesses, placing it in the upper-middle section of the global ranking with a score of **54/100**. The persistence of unresolved issues within the national landscape has heavily penalized the country's international perception. Elements such as the prolonged absence of an organic regulation concerning **lobbying** and the partial blurriness of borders between public and private interests contribute to eroding the solidity and impartiality of the Public Administration.

**FOCUS**

**The "Qatargate" Scandal, 2022**

The vulnerability of institutions does not spare the supranational European level, as dramatically confirmed by the judicial investigations into the case known as **Qatargate**. The forensic inquiry, which involved the operational collaboration of MEPs, former MPs, and assistants of Italian origin, unveiled a complex circuit of **bribe exchanges, international corruption, and money laundering** orchestrated by third States to unduly condition political decisions, geopolitical resolutions, and economic orientations of the European Parliament. This scandal dealt a heavy blow to the reputation of Euro-unitarian democracy, confirming the urgency of introducing strict technological barriers, mandatory transparency registers, and proactive controls over the financial flows of public decision-makers to protect the Union in a phase of severe geopolitical complexity.

## II. Which Provisions Allow the European Union to Protect Its Financial Interests?

The protection of the **financial interests of the European Union (PIF)** and the repression of fraudulent or corrupt behaviors affecting the community budget constitute a matter of a complex nature, characterized by a distinct shared and transnational competence. The functioning of the Union depends on the certainty of its revenues (traditional own resources, customs duties, VAT quotas) and the correct allocation of its expenditures (structural funds, recovery funds). Consequently, enforcement action is directly safeguarded by the primary sources of the European Treaties, which impose precise obligations of advanced criminal protection on Member States.

**REFERENCES**

**TFEU, Art. 310 para. 6 and Art. 325**

**Art. 310, para. 6 of the TFEU** sets out the core principle of sanctioning solidarity: "The Union and the Member States, in accordance with Art. 325, shall counter fraud and any other illegal activities affecting the financial interests of the Union". This duty of protection is analytically detailed by **Art. 325, para. 1 of the TFEU**: "The Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through measures to be taken in accordance with this article, which shall act as a deterrent and be such as to afford effective protection in the Member States, and in all the Union's institutions, bodies, offices and agencies."

Preventive and ex-post oversight over the lawfulness and regularity of these massive financial resources is entrusted to the vigilance of the **European Court of Auditors**, which formally holds the rank of one of the seven institutions of the Union. On the plane of substantive criminal law, the milestone harmonization legislative act is constituted by **Directive (UE) 2017/1371 (PIF Directive)**, adopted in implementation of **Art. 83, para. 1 of the TFEU**, which qualifies **corruption** and **money laundering** as Eurocrimes equipped with a distinct cross-border dimension, legitimizing the setting of minimum definitions and common sanctions within the Area of Freedom, Security, and Justice.
The PIF Directive specifies that fraudulent conducts can harm the Union budget both from the expenditure side (e.g., illicit capture of agricultural or structural funds through document falsification) and from the revenue side, introducing for the first time the criminal harmonization of **serious fraud against the common system of Value Added Tax (VAT)**, provided that the offense is connected to the territory of two or more Member States and determines a total financial damage of **at least 10 million euros**.

Transnational investigative practice highlights a precise dogmatic breakdown of these tax frauds that we must memorize:

- **Intra-community Operator Fraud (Carousel Fraud):** It is configured as a sophisticated evasion circuit wherein a legal entity imports goods under a VAT exemption regime from one Member State, to then resell them on the internal market of another Member State, regularizing and collecting VAT from the final customer. The entity responsible for the importation and the first national sale is termed a **"missing trader"**, who pockets the VAT paid by the buyer and systematically vanishes, omitting its payment to the state treasury and disappearing from the market before the financial administration can activate tax assessment and collection procedures.
- **Missing Trader Fraud and the Reaction of the Commission:** This specific method of evasion inflicts severe direct asset damage on the treasuries of Member States and, consequently, on the quota of own resources due to the European Union. The *VAT Action Plan* of the European Commission highlights how such conduct vulnerabilities tax efficiency, distorts competition, and requires real-time monitoring of customs flows.
- **VAT Fraud Managed by Structured Criminal Organizations:** This constitutes the hypothesis with the highest coefficient of criminal disvalue, configuring a severe aggravating circumstance of the crime. In this transnational offense, criminal cartels do not limit themselves to using a single missing trader, but structure a commercial supply chain composed of **multi-layered shell companies and "filter" companies (shell or *buffer* companies)**. These intermediate legal entities repeatedly exchange invoices for non-existent transactions and fictitious tax documents for the sole purpose of **fragmenting and obscuring the traceability of financial operations**, eluding the cross-checks of the various national jurisdictions involved and obstructing the forensic investigations of the European Public Prosecutor's Office (**EPPO**).

The **Repressive Architecture of Carousel Fraud Between Criminal Network and Technology** is articulated into four phases

- **Phase 1 - Intra-community Purchase (VAT Exemption):** Company A (located in Member State 1) sells and dispatches goods to Company B ("Missing Trader", located in Member State 2) under a cross-border VAT exemption regime.
- **Phase 2 - Sale on the Internal Market and Collection of Tax:** Company B (Missing Trader) immediately resells the goods on the national market of State 2 to Company C ("Buffer" or filter company), regularizing and collecting VAT from the buyer, but omitting payment to the treasury and vanishing from the market.
- **Phase 3 - Multi-layered Filter and Investigative Elusion:** Company C ("Buffer") resells the goods to a Company D, issuing cascading invoices to obstruct the identification of the fraud by customs and fragment the traceability of bank flows.
- **Phase 4 - Technological and Judicial Enforcement:** Economic-financial police forces and the European Public Prosecutor's Office (EPPO) utilize **Artificial Intelligence algorithms and data analytics systems of customs flows** to intercept the abnormal speed of establishment and closure of *missing trader* companies, ordering the immediate freezing of bank accounts and electronic payment channels before the drainage of illicit capital.

## III. How Does the PIF Directive Define Active and Passive Corruption?

The **Directive (UE) 2017/1371 (PIF Directive)** establishes that the prerequisite for the crime of corruption resides in the violation of the duties of diligence, good faith, fairness, impartiality, and responsibility that weigh upon public officials in the exercise of their institutional functions. From a dogmatic and criminal protection standpoint, the Directive operates a clear breakdown of conducts under Art. 4, introducing three minimum common incriminating offenses that Member States are obliged to transpose into their respective domestic legal systems:

- **Passive Corruption:** Configured as the conduct of a public official who, directly or through an intermediary, requests or receives advantages and benefits of any nature (both economic and non-patrimonial), or accepts the mere promise thereof, to perform or omit an act proper to their functions or contrary to official duties, in such a way as to damage or be capable of damaging the financial interests of the European Union.
- **Active Corruption:** Identifies the specific mirror conduct of anyone who promises, offers, or procures, directly or through an intermediary, an advantage or a benefit of any nature to a public official, so that the latter performs or omits an act in accordance with the indications provided, thereby failing in their official duties to the detriment of community resources.
- **Misappropriation:** This offense presupposes the intentionality and specific intent (*dolo specifico*) of the public official who is entrusted, by reason of their office, with the direct or indirect management of financial funds or movable assets. The crime is consummated at the moment the official allocates or uses such resources for purposes other than those originally planned and approved, in order to procure an unjust asset advantage for themselves or a third party or to directly appropriate them.

The repression and prosecution of these PIF crimes demand the application of the principles of **criminal solidarity and cross-border judicial cooperation**. National legal systems are supported by the synergistic action of special agencies such as **Eurojust and Europol** (including through the analysis of cybernetic and illicit financial flows).

Once preliminary investigations are verified and digital and documentary evidence establishing the existence of the crime is gathered, the competent bodies formally communicate the initiation of criminal proceedings to the European Commission and the Member States involved. In this scenario, a crucial and vanguard role is performed by the **EPPO (European Public Prosecutor's Office)**, an independent organ of the Union structured to work in close collaboration with delegated national prosecutors in order to coordinate and exercise criminal prosecution.

On the plane of legislative drafting and the formal process of adopting Union statutory acts aimed at protecting the budget, informal interinstitutional dialogues, commonly termed **trilogues**, acquire strategic relevance. They represent negotiation tables for exchanging views among the European Parliament, the Council of the European Union, and the European Commission, aimed at fostering a political and technical compromise prior to the formal readings of the ordinary legislative procedure.

The direct result of this consultation method was the launching of the **Interinstitutional Agreement of December 16, 2020,** concerning budget discipline, cooperation in budgetary matters, and sound financial management of the Union itself.

The agreement is permeated by a spirit of institutional cooperation aimed at supervising expenditures and conducting rigorous **administrative investigations into the improper or distorted use of European funding**. The institutions aim to promote and safeguard the regularity of financial flows within the following strategic areas of the Union:

- Urban, rural development, and regional cohesion.
- **International and emergency humanitarian aid** (with specific reference to aid granted to the population of Gaza and in support of Ukraine).
- Scientific research and university education (Erasmus+ and Horizon Europe Funds).
- Technological innovation, ecological transition, and digital inclusion.
- Employment, welfare, and social inclusion.
- Maritime policies and sustainable management of fisheries.
- Youth policies and sports development.

To this end, the European Commission operates in coordination with **OLAF (European Anti-Fraud Office)** to carry out administrative inspections on the ground. Furthermore, the fight against fraud and tax evasion is programmatically sustained by the Union through the introduction of **new own resources** of the budget (e.g., plastic tax, ETS quotas), which allow financing the resilience of Europe in the face of epochal challenges of climate change, energy transition, and digital sovereignty.

## IV. What Jurisdictional Conflicts Exist Between PIF Crimes and National Jurisdictions?

From the perspective of economic criminal law, a close structural analogy and frequent criminological convergence exist between the crimes of fraud/corruption in community funds and the offense of **self-laundering**. In both offenses, an elusive and hidden conduct is carried out by the active subject upon financial funds derived from a crime, with the ultimate purpose and specific intent of concretely obstructing the identification of their criminal origin. The crime of self-laundering is configured as a **plurioffensive** offense, as the criminal sanction aims to simultaneously protect multiple legally protected interests: the administration of justice (harmed by the masking activity), the integrity of the economic-financial system, and free market competition, which is polluted by the injection of cleaned illicit capital.

However, in the practice of transnational investigations, an insurmountable obstacle arises, defined by many jurists and lecturers as a partial **flaw in the enforcement and competence-sharing system**. The conflict manifests in investigations where the European Public Prosecutor's Office (**EPPO**) faces a concurrence of offenses: the EPPO cannot continue to exercise criminal prosecution or pursue the subsequent crime of self-laundering if the latter does not appear **directly, predominantly, and inextricably linked** to the fraud on community funds (inextricably connected competence constraint). Conversely, the EPPO undoubtedly instantiates a formidable community tool for fighting fraud and customs corruption, but **it does not possess a fully supranational structure**. It operates as a hybrid and "decentralized" body, whose European Delegated Prosecutors (EDPs) act within individual Member States by applying the procedural criminal rules of their respective national codes. The EPPO is therefore forced to suffer the limits inherent in the barriers of national jurisdictions, unable to autonomously bypass differences in trial

rites and evidence acquisition to pursue connected corporate crimes, partially limiting the maximization of financial benefit and global asset protection of the European Union.
The **competence requirement** of the European Public Prosecutor's Office in the concurrence of offenses is developed into four phases:

- **Phase 1 - Predicate Offense (PIF Fraud):** A corrupt official and a private individual divert 1 million euros of European funds destined for agriculture (Exclusive and immediate competence of the EPPO *ex* PIF Directive).
- **Phase 2 - Self-Laundering Conduct:** The private individual reinvests the illicit million euros by purchasing real estate or legal corporate shares on the national territory, obstructing the forensic identification of the money's origin.
- **Phase 3 - Legal Connection Review:**
    - If Self-Laundering is inextricably linked to the fraud on EU funds: The EPPO attracts the entire investigation (*vis attractiva*) and exercises criminal prosecution for both crimes.
    - If Self-Laundering predominantly harms national taxes or offenses: The EPPO must **decline its competence** for the self-laundering portion, transferring the file to the national Public Prosecutor's Office, fragmenting the effectiveness of the investigation.
- **Phase 4 - Limits of the Hybrid Structure:** Delegated Prosecutors of the EPPO must exercise criminal prosecution before the national judge by applying the domestic code of criminal procedure, clashing with procedural diversities and the admissibility of digital and banking evidence among the Member States.

## V. How Does the International Definition of Corruption Differ from the European One?

The crimes of fraud and corruption constitute core offenses of economic criminal law, disciplined in a parallel manner both at the European level and at the international level. Although it is possible to find profiles of distinct material similarity, the definitions provided by the two systems differ due to the diverse historical-cultural circumstances in which the offense is configured, the criminal policy objectives that the different systems intend to pursue, and the dogmatic status of the active subjects resulting therefrom.
In this regard, the **United Nations Convention against Transnational Organized Crime (Palermo Convention of 2000)** provides a precise and mandatory framework of universal incriminatory scope, focused on countering mafia infiltration into institutional circuits.

**REFERENCES**

**UNTOC, 2000, Art. 8**

Art. 8 establishes that each State Party shall adopt such legislative measures as may be necessary to establish as a criminal offense the following intentional conducts: "(a) The promising, offering or giving to a public official, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties; (b) The solicitation or acceptance by a public official, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties."

This criminal pillar found its maximum expansion and global specialization with the launching of the **United Nations Convention against Corruption (UNCAC)**, also known as the **Mérida Convention** (adopted by the General Assembly on October 31, 2003), which is configured as the first legally binding instrument of universal vocation for the systemic prevention and countering of the phenomenon of corruption.
The **UNCAC Convention** consists of a Preamble and 71 articles divided into eight structural chapters, corresponding to the programmatic objectives that the States Parties pledge to pursue:

- **Chapter I - General Provisions:** Sets the purposes of the treaty and introduces core definitions.
- **Chapter II - Preventive Measures:** Obliges States to establish independent anti-corruption bodies, codes of conduct for public decision-makers, and transparency criteria in procurement.
- **Chapter III - Criminalization and Law Enforcement:** Defines substantive offenses (corruption, misappropriation, obstruction of justice).
- **Chapter IV - International Cooperation:** Governs extradition, mutual legal assistance, and joint investigations.
- **Chapter V - Asset Recovery:** Represents the true **revolutionary and innovative profile** of the treaty, elevating the return of assets stolen through corruption into a fundamental principle of international law.
- **Chapter VI - Technical Assistance and Information Exchange:** Enhances the principle of solidarity and the development of collaborative capacity to jointly counter financial crimes.
- **Chapters VII and VIII - Mechanisms for Implementation and Final Provisions:** Regulate the application of the treaty and the submission of States to periodic reviews by the Conference of the States Parties.

Regarding regulatory criteria, the **macroscopic difference** between international discipline (UN) and European discipline (UE) lies in the level of cogenza, flexibility, and prescriptive detail of the norm.
The international UN instrument possesses a **broader, more flexible, and soft law approach**, providing general principles and recommended measures rather than rigidly binding the actions of States to extremely stringent parameters that are sometimes logistically difficult to implement. While on one hand this universal perspective may appear generic or vague, on the other hand it allows preserving an autonomous line of action for individual countries, which can adapt prevention measures to the specific circumstances of their political-cultural context. Conversely, European Union legislation (e.g., the PIF Directive) applies a **highly prescriptive and detailed model**, aimed at uniforming statutory minimum penalties. This European approach guarantees absolute certainty of the law and severely punishes the offense, but runs the risk of failing to consider disparities in instruments available to individual States or the peculiarities of their administrative systems, potentially causing slowdowns in trial prosecution if not supported by central agencies.
A further and decisive criterion of dogmatic differentiation resides not in the structure of the objective conduct of handling the bribe, but in the **subjective qualification of the natural person responsible** for the illicit behavior.

**FOCUS**

**The Subjective Status of the Crime (Public Official v. Public Servant):**

•**The International Model (UN Convention)**: Disciplines the all-encompassing figure of the **"Public Official"**. This is delineated as any natural person holding a legislative, executive, administrative, or judicial mandate of a State Party, or who exercises a public function or provides a **public service under the domestic law** and national statutes of the signatory State. The focus is centered on the nature of the state activity exercised.

• **The Community Model (Directive EU 2017/1371)**: Specifies and analytically sections the category of the **"Public Servant"**, operating a mandatory tripartition for the purpose of protecting the European budget. The Directive includes within the offense:

- The **Union Official**: Any person who has the status of an official or contractual agent hired by an institution, organ, or body of the European Union.
- The **National Official**: Any person who has the status of an official or public officer defined by the legal system of the Member State in which the action is perpetrated.
- The **Enforcement Official**: Any subject acting at the national, regional, or local level to manage, disburse, or control European funds distributed under a shared management regime.

While the European Union is founded on a principle of institutional cooperation that provides for joint and binding action between supranational organs (EPPO, OLAF), the UN Convention leaves wide room for maneuver to each State Party so that it acts according to its respective constitutional legal principles.

Finally, **Art. 10, para. 4 of the UNCAC Convention** introduces the obligation to extend criminal or administrative liability to collective entities: "Each State Party shall, in particular, ensure that legal persons held liable in accordance with this Article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions". Through this provision, the international Convention pledges to ensure that no person responsible for such economic crimes goes unpunished. However, we must highlight during examinations a **fundamental flaw**: the lack, at the UN level, of a central body equipped with supranational powers of investigative coordination and coactive judicial enforcement (elements that conversely characterize the architecture of the European Union through the European Public Prosecutor's Office) risks rendering the practical application of these international sanctions partially fragmented and ineffective on the cross-border plane.

The **investigative flow** of countering corruption functions in two main models:

- **International Model (UNCAC 2003)**:
  - Detection of fact;
  - Activation of national police authorities of the State Party;
  - Request for bilateral mutual legal assistance *ex* Chapter IV;
  - Limit: Absence of a central prosecutor (risk of stasis or national political filter).
- **Euro-unitarian Model (PIF Directive / EPPO)**:
  - Interception of anomalous financial flows on European funds;
  - Automatic and exclusive activation of European Delegated Prosecutors of the **EPPO**;
  - Simultaneous issuance of asset freezing decrees in the 27 Member States *ex* principle of mutual recognition;
  - Direct exercise of criminal prosecution;

## VI. What Substantive Sanctioning Instruments Define the Offense of Corruption Under Domestic Law?

In the Italian legal system, conducts damaging administrative transparency and public resources are severely disciplined by the Criminal Code (c.c.) and specific complementary laws. The sanctioning instruments activated following the judicial determination of these offenses articulate in a multilevel complex of **custodial penalties, civil-restitutory sanctions, administrative and disqualifying measures**, integrated by incisive preventive asset recovery measures.

From a dogmatic standpoint and penal typification, we must avoid the common error of confusing **fraud** with **swindling**. Although both offenses affect property, they present structurally different constitutive elements:

- **Swindling (Art. 640 c.c.):** Consists of the conduct of anyone who, through artifice or deception, inducing someone into error, procures for themselves or others an **unjust profit with another's detriment**. It is punished with imprisonment from six months to three years and a fine from 51 to 1,032 euros, configuring an ex-officio aggravating circumstance under Art. 640, para. 2, no. 1 if the act is committed to the detriment of the State or a public entity, including the European Union.
- **Fraud in the Exercise of Commerce (Art. 515 c.c.):** Specifically sanctions anyone who, in the exercise of a commercial activity or in a shop open to the public, **delivers to the buyer one movable thing for another**, or a movable thing different from that declared or agreed in terms of origin, provenance, quality, or quantity. The statutory penalty provides for imprisonment up to two years or a fine up to 2,065 euros, with a more severe penalty if the object of the fraud consists of metals or precious stones.

Unlike swindling, where the perimeter of active subjects is omnicomprensive, fraud in commerce strictly requires the status of a **qualified agent** (merchant) and punishes the fraudulent execution of the contract, whereas in swindling, the pre-existence of intent aimed at gaining the victim's consent through deception is what matters.

Regarding the protection of the Public Administration from mafia infiltration and transnational organized crime, the Italian legislator severely punishes the phenomenon of public officials' corruption, historically exploited by syndicates to monopolize the awarding of public procurement contracts and expenditure flows.

**REFERENCES**

**Italian Criminal Code, Art. 318 and Art. 319**

**Art. 318 (Corruption for the exercise of the function):** "The public official who, for the exercise of his functions or his powers, unduly receives, for himself or for a third party, money or other utility, or accepts the promise thereof, shall be punished with imprisonment from three to eight years".

**Art. 319 (Corruption for an act contrary to official duties):** Punishes with imprisonment from six to ten years the public official who, to omit or delay an act of his office, or to perform an act contrary to official duties, receives or accepts the promise of money or other utility.

It must be remembered that the penal status of corruption was radically rewritten by **Art. 1 of Law no. 190 of November 6, 2012 (the Severino Law)**, which overturned the sanctioning framework. The reform introduced an advanced protection threshold: in the new formulation of Art. 318 c.c., the legislator eliminated any reference to a specific

official act, punishing the mere **"sale of the public-administrative function"**. Consequently, even the single acceptance of a promise or the reception of a utility connected to the generic position of the public employee constitutes a consummated crime, operating as a powerful advanced deterrent. This framework safeguards the constitutional obligation enshrined in **Art. 54 of the Italian Constitution**, which imposes on citizens entrusted with public functions the un-derogable duty to fulfill them with **discipline and honor**.

Furthermore, the strategic link between the fight against organized crime and the protection of European economic resources found its highest operational expression in **Law no. 161 of October 17, 2017 (known as the Antoci Law)**, which reformed the Anti-Mafia Code.

**FOCUS**

**Law No. 161, 2017, and The Antoci Protocol**

The origin of this legislation lies in the proactive stance of Giuseppe Antoci, at the time President of the Nebrodi Park in Sicily, a territory vulnerable to the infiltration of mafia clans (the so-called "mafia of the pastures"). Criminal organizations used frontmen and falsified anti-mafia certifications, or bypassed controls by exploiting minimum exemption thresholds, to **illegitimately lease state-owned lands**, thereby intercepting millions of euros of European funds allocated by the **Common Agricultural Policy (CAP)**. To dismantle this illicit business, Antoci promoted a rigorous Legality Protocol, which introduced a **mandatory obligation to present anti-mafia certification for any public tender**, eliminating any minimum value exemption threshold. Extended to the entire Sicilian region in 2016, the Protocol was fully integrated by Parliament within Law No. 161/2017, becoming a law of the State applicable across the entire national territory. The European Commission officially qualified the Antoci Law as an **investigative model of excellence** in protecting the financial interests of the European Union against structured mafia crime.

The historical relationship between the Italian State and European institutions regarding community fraud was shaped by a series of judicial investigations that highlighted the necessity of a centralized and supranational cooperation.

**FOCUS**

**From *Tangentopoli* to the *Poseidone* Investigation**

**The *Mani Pulite* Investigation Cycle (*Tangentopoli* - 1992):** The investigations that led to the collapse of the so-called *First Republic* revealed an endemic system of bribes polluting public contracts. Forensic audits proved that corrupt flows involved, in part, funding allocated by European structural funds as well. The scandal pushed community institutions to launch a profound reflection on transparency, accelerating the strengthening of **OLAF's** investigative powers.

**The *Poseidone* Investigation (2005):** Conducted by the Calabrian judiciary, the investigation unveiled a massive system of **diversion and improper use of European funds** originally intended for the construction of water purification plants and environmental infrastructures in the Calabria region. The inquiry assumed a strong institutional and European relevance because high-level political figures seconded to Brussels institutions were among the suspects, highlighting the risk that local corruption could penetrate community decision-making dynamics, accelerating the push toward the establishment of an independent European Public Prosecutor's Office (**EPPO**).

Mafia penetration into European structural funds follows flexible and industrial operational models, as confirmed by the most relevant operations of the Italian judicial police:

- **Operation Spartacus (2010):** A historic maxi-trial that crushed the leadership of the Camorra-style *Casalesi clan*. Economic-financial investigations coordinated by the DDA demonstrated how the mafia organization had capillary infiltrated the allocation procedures of **European funds for rural development**, diverting clean capital to finance parallel illicit activities, such as controlling the cement cycle and illegal extraction of inert materials in the province of Caserta, thereby distorting the rules of the common market.
- **The Araba Fenice Operation (Siracusa):** This investigation hit a strategic funding sector different from the environmental or agricultural compartments, namely the management of **European Structural Funds**, with specific reference to the **European Regional Development Fund (ERDF)**, implemented by the Union to upgrade healthcare, energy, and educational infrastructures for the local population, thereby reducing regional disparities. Aggravated swindles against the State and the EU were systematically executed through the issuance and declaration of **falsified or "inflated" invoices**, where the accounting gap between declared expenses and actual site costs turned into a net profit for the criminal organization. Parallelly, falsified reports were filed by complicit and corrupt public officials to certify the progress of projects partially executed on the ground but, in reality, never completed.

**FOCUS**

**European Court of Auditors, Special Report No. 06, 2019**

These serious episodes of Italian judicial practice fall entirely within the definition of fraud (or fraudulent irregularities) provided by the European Court of Auditors in its Special Report no. 06/2019. The institution defines PIF fraud as: "any intentional action or omission, use or presentation of false, inaccurate or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds from the general budget of the European Communities or budgets managed by them, as well as the diversion of such funds for purposes other than those for which they were originally granted".

The economic impact of these illicit conducts on the budget and cohesion programs of the European Union highlights a financial vulnerability of macroscopic character. According to official data analyzed within the PIF Report (Protection of the Financial Interests) regarding fraudulent irregularities registered in each financed sector during the five-year period examined by the Court of Auditors and the Commission, a clear concentration of the criminal threat emerges on two pillars of the EU budget:

- **The Agricultural Sector (Common Agricultural Policy - CAP):** Catalyzes approximately **50% of the total number of fraudulent irregularities** reported at the community level. This massive penetration of fraud has diverted and compromised public resources for a total of **350.9 million euros**.
- **Cohesion and Regional Development Policies:** Represent the sector with the highest absolute economic damage coefficient. The European Union registered overall financial losses worth **1,063.6 million euros**. This massive figure constitutes **72% of the overall total of European funds compromised by fraud**, registering a value equal to three times the entire damage suffered by the agricultural compartment.

The illicit activities perpetrated in these strategic sectors determine a dual destructive effect: in the first instance, they erode and damage the financial interest and stability of the European Union budget; in the second instance, they invalidate the primary political objective of supporting the population, improving welfare services, and modernizing the territories of Member States. The economic profit accumulated by criminal cartels ends up weighing directly on the social fabric, on families, and on the credibility of national institutions, which are perceived by public opinion as insecure, permeable, and incapable of stemming systemic corruption. In the regions of Southern Italy, omitted vigilance causes a conspicuous quota of funding originally intended to strengthen infrastructures and community services to be definitively diverted by local mafias and never recovered.

**FOCUS**

**The Accreditation of "Risk-Prone"**

Following the inspections and deep economic-financial investigations conducted by the European Court of Auditors and OLAF, Italy is formally qualified as a beneficiary at high geopolitical and administrative risk, due to the high number of irregularities suspected of fraud affecting European expenditure flows. Community doctrine uses the technical expression **"risk-prone country"** in these cases. This security classification highlights the distinct vulnerability of a bloc of Member States – which permanently includes **Italy, Greece, Bulgaria, Romania, and Hungary** – registering a partial helplessness or structural weakness of national administrations in timely detecting, isolating, and sanctioning corruptible subjects and conflicts of interest nested within local bureaucratic apparatuses.

## VII. What Legislative Phases Produced the European Regulations Currently in Force Regarding Enforcement?

The current regulatory architecture of the European Union for protecting its resources and countering corrupt conduct is the result of a long **historical-institutional evolution**. In the aftermath of the Second World War, the European Coal and Steel Community (ECSC, 1951) was born with the political objective of placing the markets of these strategic raw materials under the authority of a supranational body, making a new armed conflict between France and Germany materially impossible, according to the pioneering vision outlined by the **Schuman Declaration of May 9, 1950**.

However, the original community structure did not provide the institutions with an autonomous financial budget, with the result that funding depended exclusively on the political will of Member States to pay direct contributions. The fundamental turning point occurred following the **Hague Summit of 1969**, during which European leaders decided to initiate the overcoming of this intergovernmental constraint, committing to pursue an Economic and Monetary Union. Despite the historical reticence of Gaullist France, from 1970, with the adoption of the fundamental **Council Decision 70/243/ECSC, EEC, Euratom**, the Union was formally provided with a structured system of **own resources**, aimed at guaranteeing the self-financing and strategic independence of the community budget.

This supranational fiscal system aimed to make the organization autonomous through a budget composed of:

- Common customs duties applied to extra-UE goods at external borders.
- Agricultural levies and co-participation quotas on revenues related to the Value Added Tax (VAT).

- A uniform rate applied to the **Gross National Income (GNI)** of each Member State, introduced later as a balancing resource.

Starting from the mid-1980s, a constant process of revision of the Treaties was initiated, which imprinted on the Union its contemporary political and economic strength. Under the impulse of the Commission Presidency of **Jacques Delors**, decisive steps were taken with the entry into force of the **Single European Act on July 1, 1987**, aimed at achieving the single market by 1992 through the full freedom of movement of goods, services, capital, and people. Parallelly, the budget *reres*-forms known as the "Delors I Package" were launched, intended to reduce regional socio-economic disparities through the structured allocation of structural funds.

The collapse of the Berlin Wall in 1989 accelerated German reunification. To embed the rebirth of Germany within a project of deep integration and prevent geopolitical imbalances, the German government agreed to sacrifice the historical monetary sovereignty of the mark to give life to a single community currency. Thus was born the **Maastricht Treaty (Treaty on European Union - TEU)**, signed on February 7, 1992, which imposed on Member States a rigorous path of macroeconomic convergence and financial stability, also conceived as a safeguard and guarantee in view of the future enlargement to the countries of the ex-Soviet East.

**FOCUS**

**The Maastricht Financial Convergence Criteria**

In order to access the third stage of the Economic and Monetary Union and adopt the euro, the Treaty imposed on Member States compliance with five rigorous economic parameters, which we must remember:

• **Deficit/GDP Ratio**: An annual public deficit (negative difference between State revenues and expenditures) **not exceeding 3%** of the Gross Domestic Product.

• **Debt/GDP Ratio**: An overall total public debt **not exceeding 60%** of GDP (a parameter for which Italy obtained a flexible interpretation based on the reduction trend, since national debt already stood around 110%).

• **Price Stability (Inflation Rate)**: An inflation rate not exceeding by more than 1.5 percentage points that of the three best performing Member States in terms of price stability.

• **Long-Term Interest Rates**: Nominal long-term interest rates not exceeding by more than 2 percentage points those of the three best performing Member States.

• **Monetary Stability:** Respect for the normal fluctuation margins provided by the narrow band of the **European Monetary System (EMS)** for at least two years, without devaluing one's currency against the ECU.

A further and definitive consolidation occurred with the signing of the **Lisbon Treaty on December 13, 2007**, which overcame the crisis of the European constitutional project. The subsequent global economic-financial crisis of 2008, however, highlighted the fragility of this framework and the partial absence of a common identity in the face of asymmetric shocks, triggering a fault line between high-deficit Southern European countries (provocatively defined by markets with the acronym PIGS) and the fiscal hawks of the North (Netherlands, Germany, Scandinavia), reluctant to grant bailout funds without the imposition of rigid austerity policies.

The European Treaties, arising from the changes introduced in Lisbon, contain stringent special provisions on budget matters. The Council of the European Union, deliberating **unanimously** according to a special legislative procedure and after consulting the European Parliament, adopts decisions on the Union's own resources, which require the formal approval of all Member States in accordance with their respective constitutional

requirements. This "quasi-constitutional" procedure requiring unanimity is strictly provided for matters of high sovereign sensitivity (parified to the provisions for the election of Parliament by direct universal suffrage or the Statutes of the members of the Court of Justice). With the same special procedure, but after obtaining the **consent** of the European Parliament, the Council adopts the regulation fixing the **Multiannual Financial Framework (MFF - Multiannual Financial Framework)**.

**REFERENCES**

**TFEU, Art. 312**

Art. 312, para. 3 of the TFEU establishes the technical function of the multi-year budget: "The financial framework shall fix the amounts of the annual ceilings on commitment appropriations by category of expenditure and of the annual ceiling on payment appropriations. The categories of expenditure, limited in number, shall correspond to the Union's major sectors of activity". The MFF ensures the orderly progress of the Union's expenditures within the limits of its own resources for a period of at least five years (ordinarily fixed at seven years, as in the current 2021-2027 cycle).
Within this multi-year financial programming framework is placed – as analyzed in previous paragraphs – the **Directive (UE) 2017/1371 (PIF Directive)**. It constitutes the criminal instrument par excellence of the European Union, designed to typify in a detailed manner offenses against the budget, imposing on Member States the adoption of uniform repressive measures to protect funds allocated by the MFF from corrupt conduct and systemic fraud.

The **historical progression of European budget reforms** can be synthesized into four phases:

- **Phase 1 – ECSC (1951):** Absence of an autonomous community budget; total dependence on direct and discretionary contributions paid by individual Member States.
- **Phase of Own Resources (Decision 70/243):** Establishment of financial autonomy through common customs duties, agricultural levies, and VAT revenues. The need arises for centralized controls entrusted to the **European Court of Auditors**.
- **Phase of the Single Market and Parameters (Maastricht 1992):** Establishment of structural funds (Delors Package) and fixing of rigorous financial convergence criteria for deficit (3%) and debt (60%).
- **Phase of Today's Codification (Lisbon / PIF Directive 2017):** Institution of the Multiannual Financial Framework *ex* Art. 312 TFEU under conditioned majority/unanimity and launch of Directive 2017/1371 for criminal harmonization of corruption and transnational fraud offenses on community funds.

## VIII. Which Historical Cases Marked the Institutional Evolution from UCLAF To OLAF?

The path of the European Union toward structuring an advanced system for preventing and suppressing corruption and fraud has been punctuated and accelerated by **severe institutional crises and emblematic rulings** of the Court of Justice of the European Union (CJEU). These cases of practice demonstrated how control deficits and opacity in decision-making processes could compromise the very credibility of the community project, fueling euro skepticism and imposing structural reforms of historic proportions.

**FOCUS**

**The Collapse of the Santer Commission and the Institutional Crisis of 1999**

The most notorious and disruptive political scandal in the history of the Euro-unitarian executive is represented by the allegations of **fraud, nepotism, and mismanagement** that engulfed the **Santer Commission in 1999**. Investigations by a committee of independent experts highlighted widespread irregularities in fund management and the assignment of consultancy contracts to family circles by certain commissioners. Regarding the political dynamics within the European Parliament, an intense debate took place: the Group of the Party of European Socialists (PES) took an intransigent line of action against the commissioners, including those from their own political orientation. This strategic choice responded to the need to avoid political isolation and preserve the party's credibility, transmitting an image of absolute transparency. At the same time, the move aimed to exert such pressure as to force the entire Commission, led by Jacques Santer (an exponent of the European People's Party), to resign.

In the historic votes of January 14, 1999, the European Parliament expressed itself in favor of the line promoting the principle of **collective responsibility of the members of the Commission**, pursuant to what is today enshrined in **Art. 234 of the TFEU**. Although it did not reach the formal vote of a motion of censure (no-confidence) to avoid a constitutional and institutional trauma in an era already marked by complex negotiations for enlargement to the East and the introduction of the euro, the Assembly induced the entire Santer Commission to tender their **voluntary resignations en bloc on March 15, 1999**, a unique event in the history of the Union.

This scandal produced a wave of strong distrust in public opinion, which began to perceive the EU as an excessively bureaucratic, clientelistic system permeable to crime, dealing a severe blow to the sentiment of common identity. To stem the euro skeptical drift, the institutions launched radical transparency reres-forms. The most relevant and fruitful consequence was the liquidation of the old Anti-Fraud Coordination Unit (UCLAF) – which, depending directly on the General Secretariat of the European Commission, suffered from an obvious deficit of autonomy – and the establishment, through **Commission Decision 1999/352/EC, ECSC, Euratom**, of **OLAF (European Anti-Fraud Office)**. OLAF was born as an organism equipped with a status *sui generis*, provided with an **investigative and supervisory mandate to be exercised in full administrative independence** to protect community financial interests from any internal fraud or corruption within the institutions.

**FOCUS**

**The "Eurostat" Scandal and Double Accounting, 2003**

About eight years after the 1999 crisis, the executive's reputation was again shaken by financial investigations hitting **Eurostat**, the official statistical office of the European Union. OLAF's inquiries unveiled a systematic diversion of community funds (estimated between 4 and 5 million euros) operated by high-level officials through the signing of inflated contracts with **external shell companies**. These front entities received payments channeled into secret bank accounts and registered through a system of **parallel double accounting**, specifically structured to be invisible to ordinary controls by internal auditors and the European Court of Auditors. Following the scandal, three senior directors of the Directorate-General were relieved of their duties and prosecuted, confirming the danger of abusing top positions for the exfiltration of sensitive information and the diversion of PIF resources.

Alongside OLAF, the management of these crises historically triggered a profound process of **empowerment (strengthening) of the European Parliament**, allowing it to evolve from a merely advisory body to a central co-legislator actor. This path, initiated by the Amsterdam Treaty of 1997 (which expanded the co-decision procedure and introduced Art. 7 of the TEU to sanction States violating fundamental values), found its definitive fulfillment with the **Lisbon Treaty**. Lisbon stabilized the **Ordinary Legislative Procedure**, extended binding approval powers (consent) on Treaties, and

granted Parliament **full decision-making parity with the Council regarding the approval of the community budget**, restoring democratic and transparent control over resources. Conversely, the persistent climate of distrust fueled by these monetary scandals prompted German Foreign Minister Joschka Fischer to promote the grand project of a **European Constitution** aimed at bringing institutions closer to citizens and securing the Union's values; however, international crises and the trust deficit decreed its definitive failure during the ratification referendums of 2005.
From a strictly jurisprudential perspective, the process of emergence and contrast of these financial offenses was guided by historic rulings of the Court of Justice:

**CASE STUDY**

**Cort of Justice of the European Union, Commission v. United Kingdom, 2022**
In this fundamental ruling, the Court of Justice of the European Union solemnly condemned the defendant State for failing to adopt appropriate customs and control measures to prevent the entry into the single market of massive flows of undervalued goods (textiles and footwear), causing a colossal evasion of customs duties. The CJEU strongly reaffirmed that the action of individual Member States must develop in absolute compliance with the duties of **sincere cooperation, mutual information, and sanctioning solidarity** toward European institutions, in order to protect the integrity and correct collection of the system of own resources of the common budget.

**CASE STUDY**

**Court of Justice of the European Union, ANAS v. Ministero delle Infrastrutture e dei Trasporti, 2023**
An immediate operational impact on the Italian national legal system is found in the judgment delivered in 2023 in the litigation between ANAS and the Ministry of Infrastructures and Transport. Here, the judges examined the **administrative and criminal liability of public officials** involved in certified corrupt and fraudulent phenomena perpetrated within the management of procurement tenders. In perfect adherence to the principles of severity and dissuasion imposed by the **PIF Directive (2017/1371)**, the ministerial authority ordered the immediate **revocation and full recovery of public funding already granted**, due to the emergence of overt acts of corruption in the procedure for awarding a large infrastructure contract co-financed by the European Union through the **European Regional Development Fund (ERDF)**, confirming the effectiveness of the combination of domestic criminal sanction and Euro-unitarian property protection.

Here we synthetize the impact of crises on the Union's anti-corruption architecture:

- **The Crisis of the Santer Commission (1999):**
  - Unveils the political vulnerability of the executive;
  - Determines the historic transition from internal control of the Commission (**UCLAF**) to the investigative independence of **OLAF** (Decision 1999/352).
- **The Eurostat Scandal (2003):**
  - Highlights techniques for diverting funds through double accounting and shell companies;
  - Imposes the strengthening of auditing systems and the push toward a central Prosecutor.
- **The Lisbon Treaty:**
  - Reacts to the democratic deficit and euro skepticism;

  - Confers on the **European Parliament full co-decisional control over the budget** (MFF) and stabilizes the ordinary legislative procedure.
- **The Jurisprudence of the CJEU (C-213/19 and Anas 2023):**
  - Fixes the principle of sincere cooperation in the collection of own resources and legitimizes the immediate **revocation of Structural Funds (ERDF)** in the presence of national corruptive infiltrations.

## IX. How Do Specialized European Agencies Practically Operate in Combating Public Corruption?

The operational framework for protecting the financial interests of the European Union (PIF) rests on a complex, multilevel system of integrated control. This structure effectively connects domestic law enforcement and monitoring bodies with independent supranational agencies, blending administrative inspections, criminal intelligence, and direct judicial prosecution.
The primary institution invested with top-level financial auditing is the **European Court of Auditors**. It analytically examines the legality and regularity of all revenue and expenditure of any body, agency, or institution connected to the Union, ensuring compliance with the requirements of sound financial management.

**REFERENCES**

**TFEU, Art. 287**
Art. 287, para. 2 of the TFEU defines the investigative competence of the body: "The Court of Auditors shall examine the operational accounts of all revenue and expenditure of the Union. It shall also examine the accounts of all revenue and expenditure of all bodies set up by the Union insofar as the relevant constituent instrument does not preclude such examination. The Court of Auditors shall provide the European Parliament and the Council with a statement of assurance as to the reliability of the accounts and the legality and regularity of the underlying transactions". The Court thus performs a vital preliminary function in detecting and bringing to light fraudulent behaviors, forwarding special reports and alerts to competent institutions.

Following the administrative auditing of the Court, on-the-field investigation is entrusted to **OLAF (European Anti-Fraud Office)**, established by Commission Decision 1999/352/EC. OLAF operates with absolute independence, gathering intelligence and conducting administrative inquiries to identify systemic vulnerabilities in the budget. It formalizes its findings in annual PIF Reports, which categorize fraud risks and guide the operational priorities of the **EMPACT** platform. Under the PIF Directive, Member States are legally mandated to transmit all detected financial irregularities to OLAF.

**FOCUS**

**Operation "Mala Gestio", 2013**

A prime example of how European investigative authorities cooperate with national judicial police to crush the diversion of EU funds is represented by **Operation Mala Gestio**. The inquiry, coordinated by OLAF on an informational level and executed on the ground by the Economic-Financial Police Unit of the **Guardia di Finanza of Palermo**, dismantled a criminal syndicate responsible for the illicit reception of **15 million euros from the European Social Fund (ESF)**. The capital, originally allocated to fund professional training courses and apprenticeships for unemployed citizens, was systematically drained by the perpetrators with the complicity of corrupt public officials inside the local Public Administration. The dirty money was funneled through a network of fictitious **shell companies (buffers)** to conceal its origin, connecting this conduct directly with the Eurocrime of **Money Laundering**.

On the front of **customs fraud –** transnational offenses that strike the revenue side of the budget through smuggling, false declarations of origin, or fictitious tariff classifications of goods to evade customs duties – OLAF urges Member States to apply the principle of information, launching Joint Customs Operations (JCOs) in high-risk commercial sectors. This coordinated action is financed and technologically reinforced by the **Union Anti-Fraud Programme (UAFP)**.

**FOCUS**

**The Three Operational Pillars of the UAFP Antifraud Programme**

The UAFP promotes the protection of the Union's financial interests by providing Member States with targeted financial, technical, and judicial support, structured around three core IT components:

- **AFIS (Anti-Fraud Information System):** A secure, centralized IT platform that provides the technical infrastructure for the **real-time exchange of customs data** and mutual administrative assistance in agricultural and commercial fraud monitoring.
- **Hercule Programme:** Provides direct financial grants and funding for the procurement of **high-tech forensic equipment** for law enforcement and customs (e.g., container x-ray scanners at major ports, financial data analytics software, and digital surveillance devices), as well as specialized training courses.
- **IMS (Irregularity Management System):** A secure electronic reporting system that centralizes the cataloging of all irregularities and suspected fraud cases communicated by Member States, facilitating statistical data matching with third countries and external auditing organizations.

The Union's anti-fraud architecture achieved a historical milestone with the full operability (in June 2021) of the **EPPO (European Public Prosecutor's Office)**, the first independent judicial authority equipped with the power to exercise criminal prosecution directly before the national courts of participating Member States.

**REFERENCES**

**TFEU, Art. 86**

Art. 86, para. 1 of the TFEU establishes the legal basis for the office: "In order to combat crimes affecting the financial interests of the Union, the Council, acting by means of regulations in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust. The Council shall act unanimously after obtaining the consent of the European Parliament".

The EPPO was formally established through **Regulation (UE) 2017/1939**, which defines its organizational structure and jurisdictional boundaries, linking directly with the core offenses harmonized by the PIF Directive (2017/1371). We must memorize the **two-level independent structure** of this judicial organ:

- **The Central Level (Supranational Strategic Level):** Headquartered in Luxembourg, it is managed by the **European Chief Prosecutor** (a position held since its inception by Romanian magistrate Laura Kövesi), assisted by two Deputy Chief Prosecutors. The Chief Prosecutor forms, together with one European Prosecutor from each participating Member State, the **EPPO College**, which is in charge of defining the strategic guidelines and harmonizing criminal prosecution policies. The central office also houses the **Permanent Chambers** (each composed of three members), which monitor and direct field investigations, making final decisions regarding bringing an indictment, reassigning a case, or dismissing a file.
- **The Decentralized Level (Domestic Operational Level):** Composed of the **European Delegated Prosecutors (EDPs)** operating directly within the territory of each participating Member State. EDPs integrate national prosecutor offices and hold exclusive competence to launch material inquiries, order searches, request asset seizures, and prosecute cases in court. In the exercise of their PIF duties, EDPs are **completely free from any binding link, subordination, or instruction from national political or judicial authorities**, answering exclusively to the central Permanent Chambers in Luxembourg. Cases are ultimately tried by national criminal courts, without prejudice to the competence of the CJEU to issue preliminary rulings to ensure the uniform application of EU law.

However, the operational effectiveness of the EPPO faces strict **material (*ratione materiae*) and territorial (*ratione loci*) jurisdictional limits** that create a fragmented investigative landscape:

- **Material Jurisdictional Limits:** The EPPO is exclusively competent for crimes affecting the financial interests of the Union (expenditure fraud, serious cross-border VAT fraud exceeding 10 million euros, PIF corruption, and money laundering), remaining **completely devoid of jurisdiction over national ordinary crimes**, unless they are inextricably and predominantly connected to the Union's financial dimension. Any extension of the EPPO's mandate to other serious areas of crime (such as international terrorism) requires a unanimous decision by the European Council. This sharp boundary risks fragmenting complex cross-border corporate investigations, as national corporate crimes connected to the main fraud bypass the EPPO's unified action and are sent back to local domestic prosecutors, weakening investigative continuity.
- **Territorial Jurisdictional Limits:** The EPPO's reach is rigidly restricted to the Member States that formally joined the enhanced cooperation under Regulation 2017/1939. **Currently, 24 out of 27 Member States participate**, resulting in the structural exclusion of **Hungary, Denmark, and Ireland**. This geographical asymmetry prevents the EPPO from conducting direct inquiries in those territories, creating the concrete risk that these countries may transform into safe havens for economic criminals trying to evade seizure orders. To mitigate this vulnerability, Articles 25-27 of the founding Regulation impose extended

cooperation duties with **Eurojust** and OLAF, although this mechanism faces strong operational complexities on the field.

To bridge these geographical asymmetries and extend judicial and police cooperation to all 27 EU nations and third states, specialized agencies within the Area of Freedom, Security, and Justice intervene:

- **Eurojust (European Union Agency for Criminal Justice Cooperation):** Unlike the EPPO, Eurojust **does not possess executive powers of direct criminal prosecution**, but acts as a strategic coordination hub that facilitates collaboration between national judiciaries. It supports the establishment of Joint Investigation Teams (JITs), resolves jurisdictional conflicts, and, being free from enhanced cooperation limits, successfully extends its network to Denmark, Ireland, Hungary, and extra-EU states.
- **Europol (European Union Agency for Law Enforcement Cooperation):** Assures operational and criminal intelligence support to national police forces (e.g., Guardia di Finanza) to combat drug trafficking, cybercrime, and economic organized crime.

**REFERENCES**

**TFEU, Art. 86 para. 2**

The Treaties mandate tight interoperability between the different organs: "The European Public Prosecutor's Office shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, offenses against the Union's financial interests [...]".

Europol places financial analysts and digital forensics technologies at the disposal of the EPPO to track illicit cross-border monetary transactions. In the execution of its mandate, Europol operates under the supervision of the Council of the EU (JHA - Justice and Home Affairs), to which it reports its concluded activities, while simultaneously forwarding a periodic information report to the European Parliament. The Council holds the political power to appoint top executives (including the Agency's Executive Director) and votes, in full co-decision with the European Parliament, on the financial budget of the office and any potential expansions of operational competences, as historically occurred with the 2016 reform to strengthen the fight against digital terrorism.

## X. What Geopolitical Implications Do Corruption and Illicit Lobbying Entail for Transparency Policies?

In light of the financial scandals that have hit European Union institutions, Union policies regarding integrity and public ethics have progressively evolved to neutralize new and pervasive methods of infiltration by cartels and third states. Although institutions strive to guarantee democratic and participatory access to their structures, cases occur where this openness is distorted by unregistered pressure groups, opening wide spaces for corrupt maneuvers.

From the perspective of supranational judicial practice, the most disruptive and asymmetric event is expressed by the investigation launched in December 2022, globally known as **Qatargate**. The forensic inquiry revealed that certain members of the European Parliament had accepted massive cash payments, gifts, favors, and asset advantages in

order to **illegitimately influence political decisions**, geopolitical resolutions, and economic orientations of the EU in favor of the government of Qatar.
Among the top defendants were the then Vice-President of the European Parliament, Eva Kailī, and former Italian MEP Antonio Panzeri. The criminal charges formulated by Belgian magistrates in coordination with Eurojust involved the offenses of **criminal association, international corruption, and money laundering**, leading to the seizure of approximately **one and a half million euros in cash** hidden in bags and suitcases. The scandal drew harsh criticism from non-governmental organizations (NGOs) and civil society, which accused the European Parliament of structural failure in ensuring an internal control framework capable of preventing and punishing such eversive phenomena.
Recent investigative practice shows that traditional enforcement tools do not fully fulfill the deterrent role for which they were originally conceived. This trend is confirmed by corruption and infiltration inquiries involving **lobbying groups connected to the Chinese technology multinational Huawei**. According to intelligence findings, representatives of the ICT giant allegedly funneled illicit economic advantages and promises of funding to exert undue pressure and hidden influence on MEPs, aiming to steer European legislation on 5G network development and cybersecurity in favor of Beijing's strategic interests, linking directly with the Eurocrime of **Cybercrime**.
To respond to this reputational emergency, the Presidency of the European Parliament promoted a drastic counter-reform of administrative governance.

**FOCUS**

**The Metsola 14-Point Reform Plan, July 2023**

The 14-point reform plan proposed by President Roberta Metsola introduces a complex set of prescriptive rules to secure the transparency policies of the European administration. The binding pillars of the text that we must remember include:
- **Strengthening the Transparency Register:** Mandatory and targeted screening of all interest groups (stakeholders) and lobbying networks wishing to access institutional premises.
- **Ban on Unofficial Meetings (Interdiction of Shadow Groups):** A strict ban on MEPs and assistants engaging in formal relations, meetings, or exchanges with unregistered or unofficial diplomatic representations.
- **Introduction of Cooling-off Periods:** A strict ban prohibiting former MEPs from engaging in lobbying activities at the European Parliament for a period of 24 months following the end of their mandate.
- **Code of Conduct and Accessory Sanctions:** A new, strict ethical code containing detailed behavioral guidelines, backed by automatic financial and restrictive sanctions to repress corruptive behaviors

The long-term effectiveness of this framework depends on overcoming an economic paradox: as long as the financial or statutory sanction applied is perceived by criminal cartels or sponsoring third states as negligible compared to the immense asset or geopolitical advantage gained from the violation, it will remain mathematically complex to bring the phenomenon of corruption under definitive control.

## XI. How Do "Better Regulation" Strategies Connect with The Digitalization of Anti-Corruption Processes?

Following the evolution of global public governance models, the European Union has understood that the fight against corruption and maladministration is not pursued exclusively through *ex-post* criminal sanctions, but demands a radical **simplification and transparency of the *ex-ante* legislative processes**. Emulating the Smart Regulation approach developed in the United States of America, the Union has undertaken a path of regulatory rationalization aimed at guaranteeing flexibility in the face of emerging risks, evidence-based decision-making, and total public access to information and legislative texts.

This evolutionary process led to the formulation of the regulatory agenda known as **Better Regulation**, structured through **four historical and technological phases of reference**:

- **The Genetic Phase (2002-2005):** Development of the first protocols to impose on the European Commission a mandatory obligation to perform **Impact Assessments** before proposing new directives. This phase codified the need to launch wide public consultations with stakeholders, civil society groups, and citizens' associations, allowing independent technical expertise to be gathered to shield the genesis of the norm from the opaque pressures of individual industrial cartels. In parallel, the **EUR-Lex** portal was launched, guaranteeing maximum accessibility and ease of reading of legal texts.
- **The Smart Regulation Phase (2010):** Focused specifically on improving the efficiency, effectiveness, and technical quality of Union law, introducing integrated control over the life cycle of the norm to repeal regulations considered obsolete or redundant.
- **The Return to Better Regulation (2015):** Marks a methodological turning point, aiming to make the decision-making process fully open, transparent, and traceable from the initial draft stages to the conclusion of the vote. This phase programmatically aims to reduce the bureaucratic weight of the community administrative machinery to make the regulatory framework less burdensome for citizens, businesses, and domestic public administrations, reducing the bureaucratic asymmetries where corruption often thrives.
- **The "One In, One Out" Principle (2019):** Implemented by the Presidency of the von der Leyen Commission, this parameter establishes that for any new regulation or administrative burden introduced by a Union act, an obsolete pre-existing burden in the same sector of activity must be **mandatorily repealed**, blocking regulatory hypertrophy.

In **2021**, and becoming fully consolidated over the course of **2026**, this strategy of dematerialization and transparency fused with the digital transition of the Union through the establishment of the centralized telematics platform known as **"Have Your Say"**, which works in the following way:

- Citizen/Stakeholder: Tracked digital access (Have Your Say);
- Draft Directive: Online publication of the Commission's proposal;
- Open consultation: Submission of Opinions, Critiques, and Technical Data;
- Impact assessment: Forensic Analysis by OLAF and EU Experts;
- Final legislative text: Total traceability via "Better Regulation";
    - Eradication of corruption risks;
    - Enforcement of the "One In, One Out" principle.

The digitalization and disintermediation of consultation processes via *Have Your Say* remove the ascending phase of European law from the old closed-door meetings between lobbyists and officials, creating a **permanent public audit**. This digital ecosystem, integrating with OLAF's administrative inspections and the EPPO's criminal prosecution, represents the Union's most advanced institutional response to secure transparency and bring the community closer to the structures of the European Space.

## XII. Key Findings

The scientific, historical, and regulatory analysis carried out within this paper leads to the outline of **five fundamental findings** that we must keep in mind for a complete understanding of the subject matter:

- **Budget Protection as a Subsidiary Eurocrime:** Under **Art. 83, para. 1 of the TFEU**, and in conjunction with **Art. 310 and Art. 325 of the TFEU**, corruption and money laundering affecting the financial interests of the Union (PIF offenses) are classified as particularly serious spheres of crime with a distinct cross-border dimension. This legitimizes the enactment of **Directive (UE) 2017/1371** to set common minimum definitions and eradicate eversive phenomena of political influence, as highlighted by the *Qatargate* scandal of 2022.
- **Dogmatic Classification of Conducts and VAT Fraud:** Euro-unitarian legislation operates a sharp distinction between the conducts of passive corruption (the selling of public function by an official) and active corruption, introducing criminal harmonization for **serious frauds against the common system of VAT (Carousel Fraud)** exceeding 10 million euros. These offenses, orchestrated by structured criminal networks through multi-layered grids of shell companies (*missing traders*) and filter companies (*buffers*), primarily target cohesion and regional development policies (**ERDF Funds**), eroding 72% of the total resources affected by fraud, as analyzed by official PIF reports.
- **Severity and Anticipation of Protection in the Italian Legal System:** The Italian legislator sanctions crimes against the Public Administration by differentiating aggravated fraud against the State (Art. 640 c.c.) from fraud in commerce (Art. 515 c.c.). Following the Severino Law (L. 190/2012), Art. 318 and Art. 319 c.c. autonomously punish the mere "selling of the function" of a public official in compliance with **Art. 54 of the Italian Constitution**. On the front of anti-mafia prevention, the system boasts a model of global investigative excellence represented by the **Antoci Law (L. 161/2017)**, which removes exemption thresholds and mandates anti-mafia certification to prevent the infiltration of clans into the funds of the Common Agricultural Policy (CAP).
- **Institutional Evolution Driven by Real-World Crises:** The current transparency architecture of the Union is the direct result of responses provided to serious systemic crises. The collapse of the Santer Commission in 1999 and the double-accounting scandal of Eurostat in 2003 led to the dissolution of internal controls under the Commission (**UCLAF**) and the launch of **OLAF** as a fully independent administrative inspection office (Decision 1999/352). This triggered the co-decisional empowerment of the **European Parliament** over the budget (Art. 312 TFEU). This drive translates today into the simplification agendas of **Better Regulation**, the **One**

**In, One Out** principle, and the digital auditing of the **Have Your Say** platform, aimed at tracing the legislative chain and disarming opaque external pressures highlighted by the *Qatargate* and *Huawei* cases.

- **The Operational Tandem and the Limits of EPPO, Eurojust, and Europol:** Since **June 2021**, PIF judicial protection relies on the action of the **European Public Prosecutor's Office (EPPO)**, an independent organ led by Laura Kövesi and established under Art. 86 TFEU. However, the EPPO's effectiveness faces strict **material limits** (lack of jurisdiction over concurrent national corporate crimes such as money laundering, causing investigative fragmentation) and **territorial limits** (geographical exclusion of Hungary, Denmark, and Ireland), requiring subsidiary cooperation with the judicial coordination powers of **Eurojust** and the forensic intelligence and financial tracking analyses provided by **Europol**, supported on an accounting level and by technical support programs (AFIS, Hercule, IMS) by the UAFP and the **European Court of Auditors**.

# Illicit Arms Trafficking

*by Francesco Potenza*[*]

SUMMARY: I. What is Meant by Arms and What is Their Legal Classification Under International and European Law? – II. Do Arms and Military Armaments Share the Same Regulation and How Do They Interface Within the Common Market? – III. Is There a Common Definition of Arms at the International Level? – IV. What Are the Characteristics of Arms Trafficking? – V. Where Do Arms Originate From? – VI. What Contribution do New Technologies Offer? – VII. What Counter-Strategies Have Been Undertaken by the United Nations? – VIII. What is the Regulation of the European Union Regarding Transfers of Armaments? – IX. Has the European Union Developed Strategies for Countering Illicit Trafficking?

KEY FINDINGS: Transnational dimension of the Eurocrime; The dual architecture of the United Nations; Tracking standards and forensic marking; The security derogation and EU export policies; Technological integration, internal market, and the EMPACT approach.

## I. What Is Meant by Arms and What Is Their Legal Classification Under International and European Law?

To comprehensively define the notion of an arm within the Area of Freedom, Security and Justice (AFSJ), it is essential to refer to the harmonized classification criteria developed by the European Union and multilateral treaties, which overcome the traditional asymmetries of individual national legal systems. European law categorizes these protective or offensive instruments based on their lethal potential, structural design, and ballistic operating mechanism. For the purpose of monitoring the internal civilian market and criminal prevention, doctrine and law enforcement agencies distinguish sharply between high-lethality devices (proper weapons or firearms) and instruments that, although manufactured for industrial, agricultural, or recreational purposes, can be converted into vectors of offense (improper weapons, such as forestry knives or machetes, which are excluded from the category of firearms because they lack a thermal propulsion mechanism).

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

**REFERENCES**

**The Three-Tier Classification of Directive (EU) 555, 2021**

The backbone of Euro-unitary categorization is established by **Directive (EU) 2021/555** on control of the acquisition and possession of weapons, which binds Member States to adopt a standardized classification structured around three risk classes:

- **Category A - Prohibited firearms**: Includes automatic rapid-fire devices, lethal military products, firearms camouflaged as other objects, and, following post-2015 reforms, semi-automatic firearms equipped with high-capacity magazines or derived from military platforms, the possession of which is strictly precluded for civilians, save for exceptional derogations for sporting or collecting purposes.
- **Category B - Firearms subject to authorization**: Includes semi-automatic short-barrel pistols and revolvers, as well as smooth-bore or rifled long-barrel firearms that require the issuance of a qualifying title (license or carrying permit) by national public security authorities.
- **Category C - Firearms subject to declaration**: Covers long-barrel hunting rifles and ordinary repeating devices that impose a mere obligation of declaration and insertion into electronic registries.

The architecture present in Directive (EU) 555/2021 interfaces in a comparative manner with the Italian legal system, which transposes these constraints by distinguishing between common firearms (regulated by Art. 2 of Law No. 110/1975) and compressed air or gas devices generating less than **7.5 Joules** of kinetic energy, which are declassified to free-sale instruments for adults since they lack a pronounced offensive potential. For the purposes of insertion and cross-border criminal tracking, the European Directive mandates a binding obligation of **permanent and indelible marking** on all essential components of the device (barrel, frame, slide, bolt), allowing *blockchain forensics* in the event of a seizure within smuggling circuits.

Alongside the civilian market, international law and CSDP policies isolate the macro-category of **war weapons**, defined as those instruments characterized by a deadly destructive power and designed, by engineering requirements, for the modern armament of troops and tactical warfare, including bombs, anti-personnel or anti-tank mine systems, booby traps, and chemical, biological, radiological, or nuclear (CBRN) agents. Under the profile of clandestine manufacturing, a strict penal regime strikes incendiary weapons (such as Molotov bottles and devices, classified as material of war due to their capacity to cause mass destruction at zero cost), whose asymmetric proliferation is monitored at a universal level by **Protocol III of the 1980 UN Convention on Certain Conventional Weapons (CCW)**. On the domestic Italian level, the technical verification of non-belligerence and the cataloging of legal devices are mandated by law to the **National Proof House (*Banco Nazionale di Prova*) in Gardone Valtrompia**, which operates as a ballistic certification organ integrated into the European security architecture.

## II. Do Arms and Military Armaments Share the Same Regulation and How Do They Interface within the Common Market?

Having traced the divisions governing civilian devices and individual firearms, it is necessary to analyze the special supranational statute applicable to the macro-category of **military materials and armaments**, a sector that escapes private domain to root itself in the sovereign prerogatives of States and multilevel defense alliances. Under the European criminal law and economic profile, the notion of military armament presents a conceptual

scope significantly broader than the definition of firearm in the strict sense, configuring as an integrated industrial supply chain.

**FOCUS**

**The Common Military List of the European Space**

Pursuant to **Directive 2009/43/EC** (aimed at simplifying the terms and conditions of transfers of defense-related products within the Community), the categorization of war materials is governed by a binding technical Annex, periodically updated by the Council of the European Union, which defines "**defense-related products**" on the basis of requirements or technical-construction and design features explicitly oriented to military or police use. This common list includes:

- Smooth-bore weapons and automatic weapons with a caliber of 12.7 mm or greater, and related ammunition systems.
- Bombs, torpedoes, rockets, missiles, and explosive devices and equipment specifically designed for military use.
- Armored ground vehicles, tanks, warships, and related special equipment.
- Military aircraft, attack helicopters, strategic UAV drones, and electronic warfare systems.
- IT systems or photographic and electro-optical devices designed for tactical targeting or training.

This European framework interfaces with national Italian legislation, governed by the rigid prohibitions of **Law July 9, 1990**, **No. 185**, which establishes that the characteristics of an armament must be evaluated based on intrinsic, objective, structural criteria, regardless of whether the temporary ownership of the semi-finished product lies with a private enterprise (**Court of Cassation, Penal Section I, No. 26835/2024**). The trade and cross-border transit of such armaments are exempted from the ordinary rules of free trade within the internal market by virtue of the safeguard clause of **Art. 346 of the TFEU**, which protects the essential security interests of Member States, subjecting the supply chain to a massive administrative licensing regime aimed at preventing uncontrolled proliferation and the diversion of cargoes toward high-risk jurisdictions.

**FOCUS**

**Licensing Mechanisms and Tracking of Industrial Secrets**

To balance the security of the Union with the need to consolidate the European defense industrial base, Directive 2009/43/CE introduced an innovative system of simplified administrative licenses:

- **General and Global Licenses:** Constitute the baseline rule for transfers between Member States, issued to defense undertakings previously certified by national public authorities for a **maximum period of five years**, attesting to their reliability and professional capacity to respect export restrictions.
- **Individual Licenses:** Represent an extraordinary exception, reserved for transfers presenting a higher geopolitical or public order risk, reducing the bureaucratic burden for legitimate industrial consortia.
- **The National Registry of Enterprises (*Registro Nazionale delle Imprese - RNI*):** An Italian domestic control module (held at the Ministry of Defense) that subordinates commercial operations to prior notification of contract negotiations, pursuant to Art. 9 of Law No. 185/1990, backed by up to four years of imprisonment in case of omission (a *proper crime* according to the Court of Cassation, No. 39992/2009).

This rigid double-stage scrutiny (subjective regarding operators and objective regarding operations) meets the cogent constraints of International law, prohibiting the signing of contracts and the transit of armaments toward third countries targeted by comprehensive arms embargoes decreed by the United Nations, the European Union, or the OSCE, or

toward Regimes responsible for serious violations of human rights, converting administrative customs checks into a bulwark for global stability and connecting harmoniously with the analysis of Small Arms and Light Weapons (SALW) and the Arms Trade Treaty (ATT) that follows.

## III. Is There a Common Definition of Arms at The International Level?

Having defined the categories of arms and military armaments, it is necessary to examine whether consolidated definitions exist at the international regulatory level. The **Arms Trade Treaty (ATT)** stands today as the reference conventional text regarding the trade of weapons and armaments. Analyzing Art. 2, paragraph 1 of the ATT, one identifies an applicable scope similar to that of Italy's Law No. 185/1990 yet not entirely overlapping: the text enumerates eight categories of conventional arms, encompassing battle tanks, armored combat vehicles, large-caliber artillery systems, combat aircraft, attack helicopters, warships, missiles and missile launchers, and small arms and light weapons. Of exceptional criminological interest is the category under letter h) of Art. 2, paragraph 1 of the ATT, which is dedicated to **Small Arms and Light Weapons (SALW)**. Before arriving at specific norms for personal and portable weapons, the elaboration of international bodies focused on military armaments, understood in a broader macroscopic sense, precisely due to reasons concerning the necessity to avoid the provisioning of States and regimes that intended to deploy them in conflicts, thereby violating rules of International humanitarian law. For instance, the Resolution S/RES/713(1991), adopted in 1991 by the UN Security Council to impose an arms embargo against Yugoslavia, at the moment of the dissolution of the Socialist Federal Republic of Yugoslavia when the bloody ethnic conflict began to rage, speaks laconically of “weapons and military equipment”.

The United Nations has, however, pursued valuable interventions over the years to define and distinguish arms and armaments, by virtue of disarmament and counter-proliferation initiatives against criminal and terrorist organizations led by the Organization. This is where the definition of **Small Arms and Light Weapons (SALW)**, elaborated by a specific panel of experts mandated by the UN General Assembly, is integrated. The panel of experts defines SALW by identifying three macro-categories: personal weapons (*Small Arms*), light weapons, and ammunition and explosives.

In detail, personal weapons are those intended for the individual armament of troops (pistols, rifles, assault rifles, light machine guns), while light weapons are substantially squad-served weapons or weapons mounted on light transport vehicles (heavy machine guns, grenade launchers, portable mortars, anti-aircraft guns, and anti-tank rocket launchers). The focal point of SALW is **portability**: these are weapons that can be transported and deployed by a single person or by a small group of individuals, requiring at most light and small-sized transport vehicles. The panel recognizes in this physical characteristic a fundamental distinction compared to other types of heavy armaments, making SALW an object of specific interest for terrorist groups and criminal syndicates, as well as a central node in the execution of ground military operations and urban warfare.

**REFERENCES**

**The Comparative Text of Law No. 185, 1990, and the Arms Trade Treaty**

The comparison between the definition of military armaments under Law No. 185/1990 and the Arms Trade Treaty is interesting as both regulatory texts aim at the same objective: controlling the armaments market and preventing supplies to States that employ them in unlawful actions. The scope of application is limited to transfers of weapons destined for the military market; the civilian market, is governed by separate regulations. **Art. 2, paragraph 1 of Italy's Law No. 185/1990** classifies armaments into fifteen categories: "a) nuclear, biological, and chemical weapons; b) automatic firearms and related ammunition; c) medium and large-caliber weaponry and related ammunition [...]; d) bombs, mines, rockets, missiles, and torpedoes; e) tanks and vehicles specifically built for military use; f) ships and related equipment specifically built for military use; g) aircraft and helicopters and related equipment specifically built for military use; h) powders, explosives, propellants [...]; i) electronic, electro-optical, and photographic systems or apparatuses specifically built for military use; l) special armored materials; m) specific materials for military training; n) machinery, appliances, and equipment built for the manufacture, testing, and control of weapons and ammunition; o) special equipment specifically built for military use". This framework is completed by paragraph 2, which references the Annex of products for defense under **Directive 2009/43/EC**.

Conversely, **Art. 2, paragraph 1 of the Arms Trade Treaty** states: "This Treaty shall apply to all conventional arms within the following categories: a) Battle tanks; b) Armored combat vehicles; c) Large-caliber artillery systems; d) Combat aircraft; e) Attack helicopters; f) Warships; g) Missiles and missile launchers; and h) Small arms and light weapons".

The categories adopted by the ATT from letter a) to g) are the exact ones elaborated by the **United Nations Register of Conventional Arms (UNROCA)**, to which SALW are appended. This list must be coordinated with Articles 3 and 4, which extend control mechanisms to ammunition and related structural components.

A substantial and political difference between the two definition lists lies precisely in the absence, within the main text of Art. 2 of the ATT of ammunition, explosives, and component parts. The choice not to insert them into the primary list of conventional armaments was linked to political compromises that emerged during the codification negotiations: certain major manufacturing States, including Russia, the United States, and China, considered it unfeasible to strictly monitor the global transfers of bulk ammunition, fearing massive logistical and traceability difficulties. It was thus preferred to separate ammunition and explosives from the core Art. governing the scope of the Treaty, providing for them an attenuated regime. Signatory States are bound to establish a domestic mechanism of oversight over transfers, while on the international level an "alleviated" regime applies, referencing solely the prohibitions of transfer (Art. 6) and the regulation concerning import (Art. 7). The ATT does not mandate any specific and strict multilateral procedures regarding export controls for these items, guaranteeing a significant bureaucratic relief for large producer countries, but leaving a vulnerability that illicit trafficking networks attempt to exploit.

## IV. What Are the Characteristics of Arms Trafficking?

The military industry has experienced exponential expansion since the Second World War. With the advent of the Cold War, armaments found, for geopolitical and economic reasons, channels to diffuse capillary across every geographic quadrant of the planet. Finally, the dissolution of the socialist bloc and the Warsaw Pact witnessed the influx

onto the illegal market of massive quantities of weapons and surplus military stocks, sold off by private actors and unfaithful officials to the highest bidder in local conflicts or integrated into the arsenals of transnational criminal organizations.

The global market for conventional weapons exhibits macro-economic dimensions of remarkable scale, constituting an indispensable component of GDP for many exporting countries and generating millions of jobs within the industrial sector. The contemporary scenario of **2026** is marked by the impact of two macro-criminological accelerators: the Covid-19 pandemic, which triggered a pathological surge in the demand for weapons within the domestic civilian market (fueled by the illusion among private citizens that owning a firearm enhances personal protection), and the Russian invasion of Ukraine, which forced European States to dramatically revise their defense expenditures upward, launching a period of structural rearmament, also boosted by the Hormuz Strait crisis. Under the statistical profile, data compiled by the **UNODA (United Nations Office for Disarmament Affairs)** show that already in 2019 - prior to the pandemic crisis and the Ukrainian war - global military expenditure had reached **1.9 trillion dollars**, representing a 76% increase compared to the historic low recorded in 1998 following the post-Cold War disarmament.

The analysis of illicit trafficking focuses exclusively on the sector of conventional weapons, omitting the trafficking of bacteriological, chemical, and nuclear weapons (weapons of mass destruction), whose oversight is governed by separate special treaties and whose circulation on the black market is statistically marginal. To grasp the scale of the illicit market, this financial data must be coordinated with the volume of conventional light weapons in circulation: according to estimates compiled by the **Small Arms Survey**, there are over **1,013 million small arms and light weapons** in circulation globally. The most alarming element resides in the fact that approximately **85% of this global arsenal is held by civilian subjects**. In this scenario, a primary role is played by the United States of America, whose regulatory tradition regarding the carrying of weapons finds formal constitutional protection within the celebrated **Second Amendment of the United States Constitution**.

Faced with this massive volume, criminal organizations and terrorist cells exploit numerous customs blind spots and porous borders of transit countries to feed the black market. The smuggling of weapons qualifies as an eversive commercial activity of extreme profitability: weapons are the indispensable instruments to enforce territorial control and extort wealth, prompting both mafia cartels and eversive movements to reinvest substantial portions of their illicit profits from narcotrafficking or money laundering into purchasing firearms. In studying the phenomenon, it is necessary to operate a sharp division between military armaments (battle tanks, artillery), whose production and trade remain firmly within the domain of sovereign States and registered operators, and civilian weapons (SALW), which form the primary object of cross-border illicit trafficking managed by criminal networks.

The configuration parameters of illicit arms trafficking are:

- **The Illicit Origin of the Goods:** The trade has as its object weapons that constitute the direct or indirect proceed of theft, robbery, embezzlement, or original clandestine manufacturing.
- **The Unauthorized Status of the Actors:** The operations of import, export, brokering, or cross-border transit are conducted by private actors or corrupt white-collar professionals completely lacking the necessary licenses or ministerial authorizations, or acting in open violation of international embargoes.

In the majority of practical and investigative cases, these two variants of illegality overlap stably: firearms of stolen or clandestine origin are moved, both domestically and internationally, by criminal networks lacking any legal title, who carry out this activity professionally and reap immense profits. Likewise, regarding commercial transactions and logistical transfers executed directly by state actors, any flows executed in flagrant violation of domestic statutory rules or binding international treaties are configured as illicit.

The weapons and armaments market constitutes for States a voice of primary importance within the commercial balance. Exporting countries manage these cross-border commercial relationships with extreme care, not only due to its high economic profitability, but also and above all for strategic reasons of geopolitical influence. Since the early years of the Twentieth century, the supply and transfer of weapons systems have been an integral part of the foreign policy of Governments, from West to East, and the illicit trafficking of armaments itself must be analyzed through this lens. Rather than for mere financial profit, States have historically provided - and continue to provide - weapons in violation of domestic and international norms to assist allied Governments, resistance Regimes, or national liberation Groups in accordance with specific dynamics of political influence.

Under the profile of contemporary military history, one can consider the supply of armaments destined for Ukraine, which Western Governments have maintained uninterruptedly since before the invasion of February 2022. Initially, the United Kingdom and the United States played a fundamental role in supplying state-of-the-art anti-tank weapons systems to Ukrainian forces, constituting an indispensable aid that decreed the substantial failure of the *blitzkrieg* attack launched by Russian ground forces. In particular, the defensive capability demonstrated on the field thanks to the massive deployment of Javelin portable guided missiles halted the advance of Russian armored vehicles.

If illicit or suspicious transfers are located in a dense diplomatic shadow zone, often facilitated by the application of State secrecy to shield them from the oversight of opposition parties and civil society, there are also commercial transfers that, while completely lawful and formal under the administrative profile, raise profound questions of ethics and political opportunity.

**FOCUS**

**The Debate on Military Supplies and the Case of the FREMM Frigates to Egypt**

An emblematic example for the **EU-GLOBACT** module is the supply contract signed between the Italian Government and the Arab Republic of Egypt regarding the sale of six **FREMM (*Fregate Europee Multi-Missione*)**, warships of extremely high technological and combat value produced by national shipyards. A fierce debate ignited within Italian public opinion and parliamentary chambers regarding the opportunity of executing this export program; the commercial operation took place at a historical moment when diplomatic relations between Rome and Cairo were extremely strained and deteriorated, following the tragic news events concerning the citizens Giulio Regeni and Patrick Zaki, highlighting the perennial conflict between the industrial interests of defense and the respect for human rights enshrined in Art. 11 of the Constitution and international treaties.

**CASE STUDY**

**The Iran-Contras Scandal and the Judgment of the International Court of Justice (Nicaragua v. United States)**

An example of extraordinary dogmatic relevance for students is the transnational affair denominated **"Iran-Contras"**, which is framed within the celebrated judgment delivered by the International Court of Justice (ICJ) in the case of *Nicaragua v. United States*. During the bloody Iran-Iraq war (1980-1988) - triggered by the invasion of the Iranian regions of Khuzestan and Kurdistan ordered by the regime of Saddam Hussein - the Government of Iran found itself in a state of desperate need for military material. However, following the Islamic revolution of 1979 and the dramatic diplomatic crisis arising from the seizure of the US Embassy compound in Tehran, commercial and formal relations between Washington and Iran had been severed.

In this complex geopolitical scenario, the US Administration was nevertheless interested in restoring contacts with the Islamic Republic of Iran, harboring a strong interest in the solid petroleum *export* that the country could guarantee. This led to the design of a secret scheme to supply armaments to Iran, **deliberately bypassing the arms embargo that had been voted, following the diplomatic crisis, by the United States Congress itself**. Operating behind the logistical cover provided by the Israeli Government, in 1985 the US Administration led by President Ronald Reagan approved the transfer of a hundred **TOW wire-guided anti-tank missiles**. The commercial operations enlisted the financial and brokerage support of the celebrated Saudi arms dealer Adnan Khashoggi and the Iranian entrepreneur Manucher Ghorbanifar. In the same year, later the in the same year, Iran received an additional 408 TOW missiles via Israel, corresponding secret payments for several million dollars.

The illegal supply of weapons to the Islamic Republic of Iran constituted for Washington officials an opportunity for the **parallel financing of "shadow" operations conducted in Latin America**, in accordance with the geopolitical dictates of the historical *Monroe doctrine*. In 1979, the Sandinista regime of Marxist-communist inspiration had established itself in Nicaragua, launching a policy of expropriation and nationalization of resources. The United States Government, fearing the expansion of communist influence in El Salvador, began to militarily support the *Fuerza Democratica Nicaraguense* (FDN, better known as the **Contras**). The intensity of the US intervention registered an asymmetric crescendo, moving from a mere nod of approval toward the provisioning of weapons to a true direct military support led by CIA operatives, who executed attacks against Nicaraguan military installations and deployed the **clandestine mining of the country's commercial bays and ports**.

At the highest levels of the US executive and the CIA, it was decided to channel the financial flows and proceeds from the secret sale of weapons to Iran directly into financing military operations in Nicaragua, **thereby bypassing the budgetary obligations and amendatory acts of Congress (the Boland Amendment) that strictly forbade opening spending lines in favor of the Contras**. In this way, several million dollars derived from the black market of TOW missiles were destined to provide the Contras with armaments, logistical support, tactical training, and occult funds for the recruitment of mercenaries.

Leaving aside the heavy institutional and internal political consequences that followed in the United States, the affair has assumed a fundamental dogmatic value before the **International Court of Justice**. With a landmark judgment delivered in 1986, the ICJ solemnly affirmed that the operations conducted by the United States violated Customary international law, standing in open opposition to the principle of the state sovereignty of Nicaragua. Furthermore, in rejecting the justification raised by the United States that the actions were covered by the principle of collective self-defense, the Court affirmed that the financial and logistical assistance, training, and supplying of weapons to rebel forces and paramilitary formations **constitutes a violation of the peremptory norm (*ius cogens*) of the prohibition of the use of force in international relations**, motivating the inadmissibility of self-defense with the absolute absence of a direct and actual armed threat by Nicaragua, fixing a cornerstone of international law against the illicit procurement of armaments.

As observed through the analysis of the Iran-Contras scandal, private operators perform a role of fundamental logistical and executive relevance within the trafficking of armaments. Whether private citizens acting as arms dealers and facilitators, or commercial companies offering their industrial infrastructure to conceal trafficking designed by state apparatuses, these represent essential hinge actors. While state actors are ordinarily moved by political reasons and geopolitical projection, private operators find in the pursuit of personal profit the primary engine of their economic interest. Under this profile, the black market for weapons moves a volume of business estimated in billions of dollars per year: final buyers are indeed subjects strictly cut off from legitimate commercial circuits due to embargoes, sanctions, and interdictory measures adopted by States or international Organizations, or criminal actors requiring weapons supplies that fall outside the systems of traceability made mandatory by public authorities.

The situations of chronic political instability and ethnic conflicts constitute exceptional business opportunities for traffickers. These crises not only cause an explosion in the demand for weapons lacking forensic marking, but also allow networks to directly access the arsenals and depots of those States and regimes that are dissolving: one can consider the dissolution of the Soviet Union and the rapid, uncontrolled reallocation of weapons and military surpluses of the Red Army into the civil conflicts of Central Africa and the theaters of war in the Balkans during the 1990s.

The black market is present and proliferates also within wealthy Western States, structuring operational times and modalities designed to elude the action of control authorities that are certainly more attentive and equipped with advanced investigative technologies. In areas of the world characterized by greater political and legal stability, the black market for weapons operates of itself as a potent factor of social destabilization, feeding and supporting the activities of indigenous organized crime. One can consider the massive military arsenals of cross-border origin seized on multiple occasions by police forces from *Camorra* clans or *Mafia* families, as well as the assault weapons employed for the commission of heinous terrorist attacks on European soil: in the tragic attack perpetrated in Paris against the headquarters of the newspaper *Charlie Hebdo*, the eversive hit squad effectively deployed assault rifles and war weapons of Soviet manufacture and derivation.

Criminal organizations also exploit the illicit arms market as a formidable subsidiary tool for **money laundering** and the reinvestment of dirty capital derived from other criminal activities, such as narcotrafficking. The purchase of weapons configures as a long-term patrimonial investment, which allows the acquisition of durable, non-perishable goods capable of consolidating the intimidation power of groups. Since weapons are durable goods, buyers recognize in them surrogates of value and means of investment, which can be rapidly liquidated and resold on the black market the moment the clan requires immediate financial liquidity.

Under the profile of the analysis of illicit markets, doctrine and intelligence agencies operate a sharp conceptual and structural division between the “black” market and the “grey” market for weapons:

**FOCUS**

**The Bipartition between Black and Grey Markets**

- **The Black Market for Weapons:** Identifies the proper and totally illegal circuit, within which domestic statutory norms and supranational treaties regarding ballistic control are openly and deliberately violated at every stage of the supply chain, from clandestine manufacturing to border smuggling.
- **The Grey Market for Weapons:** Defines that opaque sector where formally qualified and authorized actors interact, possessing regular commercial licenses or institutional titles to operate legally (e.g., state officials, defense enterprises registered in the RNI, accredited professionals), who trade weapons of illicit origin, alter the end-use destinations of **End-User Certificates**, or knowingly violate international embargoes and prohibitions for geopolitical ends or occult profit.

Among the two dimensions of the phenomenon, it is precisely the **grey market** that presents the greatest and most insidious challenges for investigative bodies: not only due to its massive macro-economic and financial scale, but also due to the professional qualities and status of the white-collar actors operating within it, who exploit the folds of legislations and corporate shielding to render the preventive and repressive approach of police forces extraordinarily complex.

Illicit trafficking must therefore be considered as an integral and interconnected part of the business of large transnational organizations, whose dynamic can be understood exclusively through a holistic approach. Similar to the trafficking of narcotics, the executive chain records the presence of multiple specialized intermediaries connecting the different ends of the transaction: these **"Middlemen" (brokers)** manage the logistical transfer of weapons, documentary falsification, and the concealment of transport until delivery to the final recipient.

These specialized intermediaries manage in parallel the laundering of the proceeds from sales. It must indeed be considered that many transactions are not only settled through payment in currency or cash but are also perfected through the transfer and barter of precious materials of illicit origin, such as gold or conflict rough diamonds (*blood diamonds*). One must not underestimate, in this sense, the indissoluble eversive link connecting illegal mining operations - especially in the areas of sub-Saharan Africa - with the direct financing of firearms purchases by warlords and transnational criminal groups, binding itself on the Eurocrime of money laundering and corruption.

## V. Where Do Arms Originate From?

Inquiring into the channels of origin of weapons is fundamental for understanding the dynamics regulating the clandestine market and for designing truly effective regulatory and inspection strategies. The origin of illicitly trafficked weapons, first of all, is not always originally illicit. It can indeed involve armaments legitimately manufactured and purchased, often by state organizations, which are subsequently moved in violation of domestic or international norms. Furthermore, there are cases where state arsenals are decommissioned and sold without the necessary precautions and checks on the recipients or are purchased by "convenience" companies (*shell companies*) that present only formally the legal requirements and are employed by intermediaries to immediately transfer the weapons to the final buyers, bypassing controls. These are cases typically traceable to the shadow zones of the "grey" market.

Regarding origin *strictu sensu* illicit, financial forensics and transnational criminology must distinguish five fundamental hypotheses:

**FOCUS**

**The Five Revenue Sources of the Clandestine Market**

- **Firearms derived from crime:** Originally lawful devices that are stolen from legitimate owners through theft or robbery, fenced, and injected into the black market. In these cases, the illicit origin can be wholly or partly dissimulated, reaching the point of selling weapons even to subjects entirely detached from mafia or criminal logic.
- **Weapons diverted from the destruction chain:** Ballistic material that is unlawfully abstracted and diverted from regular scrapping or deactivation processes. This is a procedure involving multiple actors, both private and state, whose deficiencies in hand-to-pass operations allow the diversion of devices that, although formally registered as destroyed or unserviceable, are relocated intact onto the black market.
- **Reactivated or modified weapons:** Devices that, after being subjected to regular deactivation, are placed back in a condition to function and fire, mechanically subverting the modifications undergone (such as the welding of the barrel or the removal of the firing pin). A similar fate concerns certain types of antique weapons that, although models of very new design, can be appropriately retrofitted to result still lethal and efficient.
- **Transformed replicas and blank-firing weapons:** Instruments that originate as simple replicas incapable of causing harm, but which are specifically modified and machined so that they can expel projectiles and utilize common ammunition. This is the case of "blank-firing" weapons (*blank firers*), purchasable freely and without particular formalities, which can be transformed into functioning weapons with mechanical processes that are rather rudimentary, such as the milling for chip removal of the barrel obstruction to allow the deployment of ordinary ammunition.
- **Weapons of artisan and clandestine manufacture:** Devices manufactured outside authorized industrial channels, devoid of patents, identification marks, trade brands, and serial numbers, resulting totally unregistered and untraceable by police databases.

Regarding this latter category, in some areas of the world (such as the border regions of Pakistan, in the celebrated district of Darra Adam Khel), true realities of similar-industrial manufacture of weapons have developed, faithfully built by replicating the most common models on the market (such as assault rifles of the AK platform or semi-automatic pistols), manufactured at extremely contained prices. These artisan productions, often tolerated at a local level because they create jobs in areas with heavily depressed economies, contribute significantly to feeding the global black market, constituting a powerful factor of political instability in areas where state authority is deficient or insufficient. The control and repression of this genus of occult manufacture are hindered by the market itself: artisanally manufactured weapons have prices significantly lower than weapons of other origin, not having to compensate for shipping costs, duties, and import licenses, altering the rules of competition and frustrating traditional disarmament efforts.

The economic analysis of clandestine artisan productions highlights a macroscopic tariff imbalance compared to industrial channels, which reflects on the capacity of penetration of illicit markets. Under the profile of financial forensics and applied criminology, an empirical finding of exceptional relevance is offered by the comparative study conducted in the specific geopolitical theater of **Nigeria**, whose analytical data - extracted from the scientific report of Matthias Nowak and André Gsell entitled *Handmade and Deadly: Craft Production of Small Arms in Nigeria* for the *Small Arms Survey* - certify the extreme economic competitiveness of artisanally manufactured weapons compared to industrial weapons of foreign origin.

Examining the tariffs, an assault rifle with automatic operational capacity (on the model of the AK-47 platform) presents a minimum local artisan production price of just 133 USD and a maximum price of 177 USD, compared to a foreign industrial cost oscillating between a minimum of 1,034 USD and a maximum of 1,330 USD. In the short weapons sector, a semi-automatic pistol (on the model of the Beretta 92 FS) is manufactured artisanally at a price between 266 and 355 USD, while the imported industrial counterpart requires an expenditure between 532 and 739 USD. Finally, for smooth-bore single-barrel shotguns (of the pump-action type), the price of local clandestine manufacture varies from a minimum of 41 USD to a maximum of 74 USD, where the official industrial channel stands at levels between 118 and 148 USD. Artisanal production of weapons, especially in recent years, has begun to find widespread and worrying commercial penetration also within countries with advanced economies, qualifying as a low-cost and high-lethality alternative to what is legally or illegally available on the traditional market.

It must finally be considered how, during prolonged asymmetric warfare or guerrilla actions, there may be the passage of hand and the diversion of entire small state arsenals or logistical depots. One can think, as a macroscopic example, of the complex military parable of **Afghanistan**, a territory that over the last fifty years has recorded the alternating on the field, first, of Soviet military forces and, subsequently, of NATO contingent forces. The weapons supplied through complex occult channels of triangulation (*Operation Cyclone*) by the United States of America to *mujahideen* rebels to counter Soviet warfare actions during the 1980s were subsequently and effectively deployed by the same groups against NATO coalition forces within the ISAF mission.

Furthermore, at the moment of the withdrawal of Western military contingents in 2021 - executive following the Doha Accords signed in 2020 between the US Administration and the Taliban junta - massive stocks of small arms, heavy ammunition, targeting equipment, and armored tactical vehicles fell directly into the hands of Taliban militias, which formally assumed the country's political leadership. Although there are, at the current state of intelligence findings, no incontrovertible evidences regarding the immediate injection of those weapons - already supplied to NATO forces and the regular Afghan army - into the global black market, one can well understand how the absolute absence of customs controls and rigorous domestic tracking systems facilitates and renders highly plausible the cross-border movement of such arsenals, in flagrant violation of international law norms.

The historically most notorious and disruptive case of mass entry into the black market of ex-ordinance weapons is represented by the fate that affected the massive arsenals of the Armed Forces of the Soviet Union, following the formal dissolution of the State in December 1991. To this day, light conventional weapons (SALW) of Soviet derivation and design constitute some of the most widespread weapons globally, qualifying as the firing instruments of choice by terrorist groups and transnational organized crime cartels to assert territorial control and launder the proceeds of illicit markets.

It is appropriate, finally, to dwell on the complex dynamics through which weapons are concretely moved toward the final buyer. As previously highlighted, a fundamental role in this chain is performed by intermediaries. Differently from other typologies of illicit trafficking, such as that of narcotics, in weapons trafficking there is not always a direct wire between the manufacturer and the final buyer, having to imagine rather a series of fragmented lines. Revenue sources are multiple and multiple are the figures managing the different stages of the movement. First of all, there are subjects managing the apprehension of weapons, meaning the diversion of the same from industrial production

lines or depots; in this stage are located also the criminal groups or agents interested in thefts, both specialized in the matter and belonging to local petty crime. Weapons are subsequently passed to fences who locate them on the black market, managing storage and cross-border transfer.

It must be taken into consideration that the movement of weapons and ammunition requires particular precautions compared to other illicit traffics, as well as heavy logistical structures capable of managing non-negligible volumes and weights. The role of intermediaries is, therefore, fundamental not only under a strictly commercial profile, to locate goods on the market and supply buyers willing to pay the highest price, but also to allow the bypassing of state controls on heavy, voluminous shipments that often require special cautions, necessary to avoid the deterioration of goods or connected catastrophic risks.

**FOCUS**

**Storage Risks and the Example of the Beirut Devastation, 2020**

One can think, above all, of the cautions connected to the transport and storage of explosive materials or chemical precursors: on August 4, 2020, a extremely violent explosion devastated the port and the Lebanese capital **Beirut**, originating from a port warehouse where several tons of ammonium nitrate were improperly and illegally stored. This is a material deployed ordinarily in agriculture but used also by terrorist networks for manufacturing improvised explosive devices (IEDs), demonstrating how the logistics of sensitive materials requires rigid protocols of traceability.

Logistical precautions are necessary also to bypass increasingly sophisticated control technologies deployed by customs and police authorities at border checkpoints. For example, the deployment of increasingly refined metal detectors and X-ray scanners, capable of returning a three-dimensional image of scanned enclosures, requires a particular "engineering" of illegal weapons cargoes, concealed behind lead shielding or inside high-density legal goods. Also, the deployment of **canine units (K9)**, effectively deployed to sniff out weapons, forces traffickers to devise alternative itineraries or chemical subterfuges to mask the scent: similarly to what happens for narcotic substances, police dogs "sniff" weapons thanks to the particular and persistent odor emitted by **chemical oils used for lubrication, cleaning, and conservation of mechanical parts** and the barrel.

The intervention of specialized intermediaries is, therefore, indispensable to guarantee logistics and cover, also under a judicial profile, to shipments of several tons. To this, are added the **documentary falsifications** necessary to accompany and cover shipments, capable of dissimulating the presence of weapons inside a standard commercial shipment (e.g., declaring them as industrial spare parts or piping) or providing the same with a false appearance of international legality through the counterfeiting of certificates of end-user (**End-User Certificates**).

**FOCUS**

**The Otterloo Ship Affair and the Corruption Network in Colombia**

The case of the vessel **"Otterloo"** testifies how weapons belonging to State armed forces can transit under the control of criminal groups, due also to the connivance of corrupt public officials. In 1999, approximately 3,000 assault rifles, of the AK-47 type, and more than two million rounds of 7.62x39 caliber ammunition, part of the arsenal of the Nicaraguan National Police, were transferred to the Colombian paramilitary terrorist organization AUC (*Autodefensas Unidas de Colombia*). The transfer originated as a lawful agreement between the Nicaraguan Police and a Guatemalan enterprise (GIR S.A) specialized in the weapons trade: in exchange for the stock of Kalashnikov rifles of older manufacture, the Police would update its arsenal with modern pistols and submachine guns of Israeli production (including mini-Uzi). The enterprise GIR S.A was represented, in the agreement, by the intermediary of Israeli nationality Shimon Yelinek, who claimed to negotiate on mandate of the Panama Police.

The weapons, having left Nicaraguan depots, were loaded onto the merchant vessel Otterloo, which was supposed to transport them to Panama, the place of delivery to the buyer. Instead of being delivered to Panama, however, the weapons were unloaded at the port of Turbo (Colombia) and from there transported via truck into the jungle, toward the bases of the AUC. In the recesses of the shipment, Yelinek concluded a second agreement with the Nicaraguan National Police for the purchase of an additional 5,000 rifles and over 17 million rounds of ammunition: an agreement that, however, did not pass to execution following the intervention of Nicaraguan and Colombian security services, which had discovered the diversion of the first shipment.

The investigations that followed, including one conducted by the **Organization of American States (OAS)**, demonstrated how the delivery to the AUC organization was rendered possible by negligent and, in some cases, intentional conduct of state officials, both Nicaraguan and Colombian. Particularly, it was ascertained how the operation was rendered possible by the corruption, by the intermediaries, of high-ranking officers and Nicaraguan and Colombian customs officials. Upon push from the Colombian Government, the OAS adopted a series of recommendations to the involved States, Nicaragua, Panama, and Colombia, as well as to all other States of the Organization to avoid future disappearances of weapon stocks and to reduce the impact of corruption in armaments matters.

The corruption of employees at the organs deputed to control and the falsification of shipping documents allowed the supply of weapons and ammunition to the benefit of the paramilitary organization FARC (*Fuerzas Armadas Revolucionarias de Colombia*) by Peruvian government officials. Several thousand AK-47 rifles and relative ammunition, sold by the government of Jordan to Peru, were air-dropped directly into the Colombian forest, near the bases of the FARC. Subsequent investigations ascertained the central role of **Vladimiro Montesinos Torres** (involved in other cases of corruption and facilitation to organizations dedicated to narcotrafficking, he was sentenced to 20 years of imprisonment for supplying weapons to the FARC), chief of the Peruvian secret services, who designed and coordinated the operation in exchange for massive quantities of cocaine, to be located on the international market.

## VI. What Contribution Do New Technologies Offer?

Technological evolution has always played a prominent role in armed conflicts, pushing toward the design of more sophisticated and powerful armaments, capable of offering a tactical advantage on the battlefield. With the advent of the XXI Century, *electronic warfare* (electronic warfare) has assumed an increasing centrality, recording at the same time the appearance of *cyber warfare*, meaning the execution of hostilities and cyber sabotages against digital infrastructures both civilian and military. Also, Artificial Intelligence (AI) finds application inside complex and multirole weapons systems, aimed

at reducing the cognitive workload for the human operator. The criminal phenomenon of ballistic smuggling has not remained isolated from this transition. It records indeed the offer, on the illicit market, of increasingly advanced weapons, but also the adoption of occult production and trade techniques making wide use of recent discoveries in the digital, cybernetic, and manufacturing fields.

Under the profile of air vector technology, a disruptive impact is exercised by the diffusion of **drones**. If UAV aircraft (*Unmanned Aerial Vehicles*) are by now, for over two decades, an integral part of the strategic arsenals of major world powers, the most recent scenarios record the appearance of **FPV drones (*First Person View*)**. Born originally for recreational and civilian purposes, characterized by modest operational and production costs, these small radio-guided aircraft (with some wire-guided variants appeared in Ukraine) have found a highly relevant application on the battlefield. Procured with extreme ease on legal commercial markets, they are modified through installing war loads to transport improvised devices, usually small bombs or mortar grenades, being deployed with devastating effects both in anti-personnel function and against heavy armored vehicles.

**FOCUS**

**The Lethality of FPV Drones and Counter-Measure Defense Systems**

These technological instruments fall perfectly within the modern concept of SALW (Small arms and light weapons), offering a significant asymmetric advantage against an extreme ease of concealment, transport, and deployment on the field, maintaining reduced unit costs in the order of a few hundred dollars. The Russian-Ukrainian conflict testifies to the lethal effectiveness of FPV drones thus modified, capable of infiltrating deep behind enemy lines and causing severe damage to logistical infrastructures and to strategic bombers valued at several million dollars.

The deployment of armed commercial drones for criminal, smuggling purposes, or for terrorist ends constitutes a concrete threat monitored by States: inside Italian law enforcement and the Armed Forces (with specific reference to the Italian Army and the Air Force) specific **specialist units equipped with anti-drone capabilities (*Counter-UAS*)** have been established, deployed to garrison sensitive institutional objectives or during large public demonstrations to intercept and inhibit the radio frequencies of hostile vectors.

On the parallel front of the clandestine manufacture of self-produced weapons, the technological transition has offered an equally significant and alarming contribution through the diffusion of **weapons manufactured via 3D printing** (commonly denominated in doctrine **"Ghost Guns"**). Tridimensional printing technology allows the fabrication, starting from a simple digital design file (e.g., CAD models or STL codes distributed in the dark nets of the *Dark Web*), of mechanical objects with complex shapes in polymeric plastic material, in reduced times and without the need to possess industrial machinery, foundries, or special workshop equipment.

The production of weapons partially or entirely manufactured in polymeric materials constitutes a reality consolidated for years in the official industrial sector (think of the extensive use of polymer frames in modern pistols like Glocks); consequently, weapons manufactured via domestic 3D printing manage to reach levels of efficiency, mechanical resistance to shooting pressures, and ballistic reliability wholly comparable to those of industrial weapons. Under the profile of internal security of the Area of freedom, security and justice, the element of maximum vulnerability resides in the **capacity of polymeric weapons printed in 3D to pass completely unobserved by traditional metal detector control systems** and magnetic checkpoints at borders or airports.

This structural characteristic of total a-magneticity, combined with the absolute absence of identification marks, trade brands, or serial numbers stamped on the frame, zeroes the ordinary channels of investigative traceability of police forces. Such a factor sustains the demand for weapons manufactured with this technique by lone wolves, eversive cells, and unfaithful white-collar workers operating in black markets, binding itself with the need to extend the obligations of the anti-money laundering system and of cooperation between FIUs also to monitoring the financial flows connected to purchasing industrial printers and plastic precursors.

New digital technologies offer, furthermore, refined and cutting-edge computer tools for logistical management and financial masking of illicit armaments trafficking. Inside the eversive value chain, intermediaries and commercial brokers are precisely those who deploy the most advanced technological instrumentation in the occult management of economic transactions and transport vectors. The infrastructures of the **Deep Web**, the immutability of the **Blockchain**, and the deployment of **virtual currencies and cryptocurrencies** (such as Bitcoin or Monero) constitute the standard instruments recently employed to strike commercial agreements, publicize clandestine weapons catalogs, and exchange massive masses of cash escaping radically from ordinary monitoring loops of banking and judicial authorities.

Artificial Intelligence (AI) is effectively deployed by ecomafias and smuggling cartels to rationalize and optimize logistical activities and material resources deployed on the field. Predictive algorithms facilitate criminal actors in the analytical study of vulnerabilities of national customs and border infrastructures through which move cargoes of weapons, but it operates also to identify in real time which States and jurisdictions offer less severe administrative regulations and more porous border controls, allowing the execution of a true strategy of **regulatory and border "Forum Shopping"**.

As widely demonstrated for other macro-criminal phenomena examined (such as corruption or money laundering), also in this juncture it turns out to be of fundamental importance, for national and supranational investigative authorities, being able to follow backward the financial traces of payments, to trace back to the sources of provisioning of traded weapons. Aware of this investigative priority of financial forensics, criminal operators prefer deploying cryptographic monetary instruments with very high volatility and anonymity, which allow fragmenting, concealing, or erasing definitively their own accounting traces during the three stages of money laundering.

In response to these insidious technological threats, new computer technologies and Artificial Intelligence itself offer today investigators and penal magistrates instruments that are equally powerful and cutting-edge.

**FOCUS**

**The Interoperability of Cooperation Agencies on Blockchain Forensics**

Starting from the interconnection of protected and shared telematics databases between multiple public authorities of different States, investigators prefer a modern investigative approach centered on the analytical study of intrinsic weaknesses of national security systems and regulatory frameworks, crossing macro-economic and social data collected over the years on the smuggling phenomenon. Transnational police and judicial cooperation agencies are particularly active in developing this integrated technological shield:

- **INTERPOL:** Coordinates the management of the global database **iARMS (*Illicit Arms Records and Tracing Management System*)**, a computer platform allowing the cataloging, identification, and immediate international tracking of firearms lost, stolen, or seized in the various smuggling theaters of the planet.
- **Europol:** Through its specialized center against organized and economic crime, deploys sophisticated Artificial Intelligence systems to analyze forensic *big data* and logs extracted from the *Deep Web*, finding occult connections, overlaps, and similarities between different police investigations led by Member States.
- **Eurojust:** Intervenes on the front of penal judicial cooperation to coordinate the action of European magistrates and prosecution offices, facilitating the transmission of encrypted digital evidence, establishing Joint Investigation Teams (JITs), and resolving cross-border jurisdiction conflicts to build multilevel counter-strategies that optimize resources and maximize repressive results.

## VII. What Weapons Counter-Strategies Have Been Undertaken by the United Nations?

The initiatives to counter the illicit trafficking of weapons undertaken by the United Nations must be divided into two distinct dogmatic categories:

- Initiatives concerning the sale of weapons and military armaments intended to equip regular troops, where States are the primary actors.
- Instruments concerning transactions of civilian weapons, aiming to prevent them from falling into the hands of criminal and terrorist organizations.

Over the years, the United Nations has developed various regulatory instruments and targeted actions to create an international framework capable of preventing commercial operations toward regimes or groups that violate human rights or commit international crimes. These are supplemented by operational cooperation activities managed by specialized agencies, most notably the **UNODC (United Nations Office on Drugs and Crime)**.

It was only after the conclusion of the Cold War, when asymmetric conflicts and political instability led to dramatic humanitarian consequences - such as the ethnic war in the former Yugoslavia and the genocide in Rwanda - that a holistic counter-strategy emerged. Initially built upon the coercive measures adopted by the Security Council under Chapter VII of the UN Charter (specifically arms embargo decrees), flexible *soft law* initiatives were promoted, including the **UNROCA (*United Nations Register of Conventional Arms*)**. The positive experience and historical consolidation of the Register, which saw a significant number of accessions and participation, played a key role in driving the political will toward a broader, binding instrument. In 2001, within the framework of the United Nations Disarmament Program, the *Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (PoA)* was adopted. This non-binding *soft law* act, utilizing a multi-level approach, anticipated the precetive

content and tracking mechanisms of the subsequent Firearms Protocol supplementing the Palermo Convention.

Regarding the transfer of heavy military armaments between sovereign States, the primary international public law regulatory instrument is the **Arms Trade Treaty (ATT)**. Adopted by the General Assembly of the United Nations on April 2, 2013, the text was opened for multilateral signatures in June 2013, entering into force internationally on December 24, 2014, upon reaching its fiftieth ratification.

**FOCUS**

**The Pillars and Risk Assessment in the Arms Trade Treaty**

The ATT, developed and structured with the technical and documentary support of the **UNODA (United Nations Office for Disarmament Affairs)**, establishes common, universal, and strict standards for international armament transfers. Under these rules, national authorities are legally bound to establish and maintain dedicated domestic control systems. The primary purpose and *ratio* of the Treaty are to safeguard fundamental human rights and minimize the risk of *escalation* in war zones by imposing absolute transfer prohibitions and codifying rigid, prior **Risk Assessment procedures**. The ATT serves as a crucial intersection between the demands of safeguarding international peace and security and the protection of human dignity, while concurrently protecting state sovereignty and the right to territorial integrity.

Under the profile of the scope of application, the commercial operations regulated by the ATT encompass material export and import activities, as well as customs transit through national territories and cross-border intermediation or *brokering* conduct.

**REFERENCES**

**Arms Trade Treaty, 2013**

Art. 6, concerning absolute transfer prohibitions, re-emphasizes the non-derogable obligation to comply with coercive measures adopted by the UN Security Council under Chapter VII of the UN Charter, highlighting the legal weight and penal binding nature of arms embargo Resolutions. Art. 6 also reaffirms the prohibition of export if the operation violates other international conventional agreements signed by the State.

The provision of greatest significance for international criminal justice is contained within **Paragraph 3 of Art. 6**, which reads verbatim: "3. A State Party shall not authorize any transfer of conventional arms covered under Art. 2 (1) or of items covered under Art. 3 or Art. 4, if it has knowledge at the time of authorization that the arms or items would be used in the commission of genocide, crimes against humanity, grave breaches of the Geneva Conventions of 1949, attacks directed against civilian objects or civilians protected as such, or other war crimes as defined by international agreements to which it is a Party".

This provision places a stringent obligation on States Parties, binding them to implement rigorous scrutiny and assessment procedures for individual commercial operations, requiring the denial of an export license if a concrete danger of violating *ius cogens* rules exists. The norm requires that the exporting State possess awareness of the illicit use (*"it has knowledge"*), a cognitive element that does not necessarily need to be current or imminent, as it is sufficient for it to fall within a framework of high probability.

What the exporting State is called upon to activate is not an enforcement action abroad, but rather the implementation of administrative and forensic standards of risk evaluation, determining based on a rule of judgment akin to the **"more likely than not"** standard that the armaments and semi-finished military goods will not be diverted or employed for illicit purposes, connecting trade transparency with global security.

Art. 6 thus imposes a triple check on transfer operations, which acts as a preliminary step before the further technical assessments required by the subsequent regulatory framework of Art. 7. In the event that one of the absolute prohibition hypotheses under Art. 6 is not clearly detected, armament export operations can only be authorized after a deeper security check.

Indeed, **Art. 7, Paragraph 1** mandates the exporting State to verify that the ballistic material or component will not be used by the importing State to undermine international peace and security or be used to commit or facilitate serious breaches of International humanitarian law, Human rights law, or to commit or facilitate transnational activities that constitute crimes under international Conventions governing terrorism or organized crime. Looking at the literal and systematic tenor of the norm, it is evident that actual, ongoing violations on the field are not required by the sources, as the mere potentiality or risk of diversion (*diversion*) is sufficient.

The exporting State is bound to assess the appropriateness of granting the authorization in light of all information available at that moment, whether provided directly by the importing State through diplomatic channels or otherwise inferred via *intelligence* activities. The final decision regarding the issuance of the license is made by taking into account the specific offensiveness of the weapons (**Paragraph 4**), as well as evaluating the implementation of appropriate risk mitigation measures agreed upon between the Parties (**Paragraph 3**), such as secure storage systems or post-delivery verifications.

Furthermore, **Paragraph 7 of Art. 7** explicitly provides that, once an export authorization has been formally granted, the exporting State retains the inalienable right and duty to re-evaluate the overall geopolitical situation should fresh indicting information emerge or a sudden change occurs in the state of facts or the destination theater. More flexible and elastic are the conventional rules governing imports (Art. 8), customs transits (Art. 9), and intermediation or *brokering* (Art. 10), which require States to establish domestic coordination and control models over logistical and financial operations, a rigor extended to Art. 11 to prevent the hijacking of shipments. Central to these ends is the obligation of documentation and periodic reporting of commercial operations, enabling effective cross-checks by the United Nations.

## VIII. What is the European Union's Regulatory Framework on Armament Transfers?

The European Union represents, much like in other major commercial sectors, one of the primary global points of reference for the manufacture and transfer of arms and armaments, given the concentration of many of the world's leading industrial and manufacturing complexes of the defense sector within its territory. The Union configures as one of the most authoritative global actors in strategies countering ballistic smuggling; in this regard, the Commission formally committed the EU policy by acceding, in 2014, to the Firearms Protocol supplementing the United Nations Convention against Transnational Organized Crime (UNTOC).
The primary sector of intervention lies within the competencies of the **Common Foreign and Security Policy (CFSP)**, although specific coordination provisions are also embedded within the framework of the common commercial policy. It is important to clarify that, regarding the regulation of the arms trade, the Euro-unitary legal order operates in clear and express derogation from the traditional general principles of the internal market and the free movement of goods.

**REFERENCES**

**TFEU, Art. 346**

The constitutional architecture of this sovereign derogation is carved into **Art. 346 of the TFEU**, which establishes in Paragraph 1 that:

- "(a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security;"
- "(b) any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which connect with the production of or trade in arms, ammunition and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes."

Consequently, rather than establishing direct, centralized criminal incrimination measures - the punitive power of which remains firmly with individual nation-states - the action of the Brussels institutions focuses on the progressive strengthening and harmonization of administrative customs supervision over exports and imports, both within intra-community trade flows and strategic transfers directed toward third countries. Working alongside this first commercial core are complementary legislative acts aimed at improving and standardizing national systems for authorization, ballistic classification, and the control of firearm possession by private citizens. Treating CFSP instruments as a priority, these provisions are designed to govern exports directed outside the Schengen area.

The first systematic initiative in chronological order was the **1998 Code of Conduct on Arms Exports**, adopted formally by the Council of the European Union. This instrument aimed to achieve a twofold strategic objective: preventing the export of arms and industrial armaments toward third countries where they might be used to wage international aggression, suppress domestic political opposition, or fuel regional instability and conflicts; and defining high common standards for the transparent management of weapons transfers by Member States, while boosting information exchange and mutual consultation channels. To implement these goals, the 1998 Code codified **eight guiding criteria** to direct national authorities in issuing export licenses.
The criteria mandated absolute compliance with embargoes and sanctions decreed by the UN or the EU, adherence to non-proliferation treaties for weapons of mass destruction,

and the total ban on anti-personnel landmines. It also required strict respect for international law principles regarding sovereignty, territorial integrity, and human rights, precluding the risk of illicit triangulations (i.e., weapons being redirected to third countries not aligned with the guiding criteria). The text introduced a notification mechanism in the event of an administrative license denial, forcing prior consultation if a Member State intended to authorize a ballistic shipment previously denied by another Union country. The 1998 Code of Conduct, however, lacked full enforcement power due to the structural non-binding nature of its provisions, remaining a mere *soft law* act. Nevertheless, the methodological efficacy of its eight criteria was historically certified by their full incorporation into subsequent binding sources.

In 2003, the Council adopted **Common Position 2003/468/CFSP on the control of arms brokering**, an act designed to prevent arms shipments from EU countries from bypassing United Nations embargoes via opaque private brokering activities, bringing broker activities under the umbrella of security criteria. Member States are called upon to closely monitor the actions of brokers operating within their territory, extending vigilance to conduct carried out abroad by brokers who are their own citizens. The Common Position requires brokering to be subjected to a prior written authorization regime issued by public security authorities, suggesting the establishment of dedicated registries for certified brokers and prescribing the application of an effective system of internal administrative and criminal sanctions.

The true pillar and European source of reference governing outward transfers is, however, **Council Common Position 2008/944/CFSP of 8 December 2008** defining common rules governing control of exports of military technology and equipment, which follows the *EU Strategy to combat the illicit accumulation and trafficking of SALW and their ammunition*. Common Position 2008/944 configures, for the first time in the Euro-unitary legal order, as a **fully integrated and legally binding** regulatory instrument for Member States regarding extra-EU ballistic exports. It adopts the historic eight guiding criteria of the 1998 Code, introducing an important qualitative evolution: the inclusion of specific elements of evaluation for each criterion allows for a harmonized application, overcoming the ambiguity of the old text and standardizing scrutiny against the industrial interests of the 27 countries.

**REFERENCES**

**Common Position (CFSP) 944, 2008, Art. 2**

Pursuant to Art. 2 of the Common Position, export authorization is conditional upon compliance with the following mandatory parameters:

- **Criterion 1:** Respect for the international obligations and commitments of Member States, in particular the sanctions adopted by the UN Security Council or those adopted by the European Union, agreements on non-proliferation and other subjects, as well as other international obligations.
- **Criterion 2:** Respect for human rights in the country of final destination as well as respect by that country for international humanitarian law.
- **Criterion 3:** Internal situation in the country of final destination, as a function of the existence of tensions or armed conflicts.
- **Criterion 4:** Preservation of regional peace, security and stability.
- **Criterion 5:** National security of the Member States and of territories whose external relations are the responsibility of a Member State, as well as that of friendly and allied countries.
- **Criterion 6:** Behaviour of the buyer country vis-à-vis the international community, as regards in particular its attitude to terrorism, the nature of its alliances and its respect for international law.
- **Criterion 7:** Existence of a risk that the military technology or equipment will be diverted within the buyer country or re-exported under undesirable conditions.
- **Criterion 8:** Compatibility of the exports of the military technology or equipment with the technical and economic capacity of the recipient country, taking into account the desirability that States should achieve their legitimate needs of security and defence with the least diversion for armaments of human and economic resources.

In addition to enforcing strict compliance with the aforementioned criteria, the Common Position mandates clear mutual information obligations among Member States, particularly when a shipment license is denied. Art. 3 explicitly preserves the right of individual States to adopt more stringent national regulations and restrictive scrutiny criteria.

The CFSP framework is complemented by **Council Regulation (EC) No 428/2009 on the control of exports, transfer, brokering and transit of dual-use items**, which covers materials, components, and technologies capable of both civilian industrial and military warfare applications. A strict customs authorization system is also established for dual-use items; however, to facilitate legitimate commercial development and technological transactions, this check is conducted without needing to subject shipments to the political evaluation of the eight Common Position criteria.

Under the profile of the strategic and industrial outlook of the European Union, regulation concerning arms and armaments within the CFSP sector is destined, in the current **2026** scenario, to take on an even greater geopolitical centrality. In 2025, the European Commission led by President Ursula von der Leyen announced a massive extraordinary investment plan for common defense. The plan, dubbed **"ReArm Europe"**, provides for the allocation of resources up to **800 billion euros** aimed at improving the tactical mobility of the Member States' Armed Forces and increasing strategic defense stockpiles, in preparation for the so-called "worst case scenario".

This plan, developed in response to constant threats posed by the Russian Federation's armed forces on the eastern front and a policy of partial isolationism by the United States under the second Trump administration, will lead to a notable increase in the industrial manufacture of arms and military equipment by European companies and consortia, with a consequent and massive increase in export volumes destined to reshape customs and boundary monitoring flows. Notably, the rearm plan has been further strengthened by the

Hormuz Strait crisis in 2026, urging the EU and Member States to allocate more financial resources to arms investments.
On the parallel front of internal markets and intra-community transfers, the Union has developed specific rules to simplify and harmonize the circulation of defense products. **Directive 2009/43/EC** of the European Parliament and of the Council of 6 May 2009 regulates exclusively the terms and conditions of transfers of defense-related products within the Union, streamlining and coordinating administrative licensing procedures. An operational system is built where the baseline rule is represented by the issuance of **general licenses** (directed at all certified suppliers within the State's territory) and **global licenses** (granted to individual industrial suppliers for their multi-year activity), while individual licenses, relating to a single and specific logistical transfer, constitute the extraordinary exception, reserved for cases of higher risk to public order, public safety, or international stability.
The special regime for transfer licenses and the correlated certification system for recipient companies indicate the consensus among Member States to remove the weapons sector from ordinary common trade rules within the community market, establishing a separate and differentiated mechanism. The certification system is established to permanently prove, for a **maximum period of five years**, the technical reliability of the recipient company, particularly regarding its professional capacity to respect export restrictions on defense products received from another Member State. Member States, in this regard, are required to designate competent public authorities for the certification of recipients established within their territory, who collaborate closely with other States' authorities to ensure traceability and prevent the diversion of cargoes toward clandestine circuits or grey markets.

## IX. Has the European Union Developed Strategies for the Prevention and Countering of Illicit Trafficking

The competence of the European Union in the area of countering arms trafficking is grounded upon **Art. 83, Paragraph 1 of the Treaty on the Functioning of the European Union (TFEU)**. This primary norm provides that the European Parliament and the Council may establish, by means of directives, “minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension” when, due to the characteristics of the phenomenon, a common and harmonized approach is necessary. However, in the specific matter of illicit arms trafficking, the Union does not directly establish penal measures - the punitive power of which is guarded by individual nation-states - focusing instead on advanced instruments centered on judicial cooperation in criminal matters and the harmonization of administrative and boundary customs regulations. As previously illustrated, while Art. 346 of the TFEU removes part of the competence over military armament trade from the Union to leave it intact with Member States, Art. 83 preserves the institution's capability to intervene in the area of countering illicit trafficking, harmonizing civilian possession and introducing broadened investigative modules.
The European Union's focus on this Eurocrime is evidenced by its formal accession to the Firearms Protocol supplementing the United Nations Convention against Transnational Organized Crime (UNTOC). The Union institutions have built a rigid regime of authorizations for the transfer and transit of weapons, both within the Area of Freedom,

Security and Justice and for commercial shipments entering and leaving the community customs space.
In implementation of the obligations assumed under the Palermo Protocol, the Union proceeded with a deep revision of its regulatory asset, repealing the old Regulation (EU) No 258/2012 to merge it entirely within the brand new **Regulation (EU) 2025/41 of the European Parliament and of the Council of 19 December 2024**.

**REFERENCES**

**The Outbound Control Regime of Regulation (EU) 41, 2025**

Regulation (EU) 2025/41 consolidates a directly applicable outbound authorization system for the civilian weapons market as well. The private exporter is required to request a specific prior authorization from the customs authorities of the Member State in which they are established. By virtue of the dictate of **Art. 7, Paragraph 1**, the authorities of the State of origin are bound to verify:

- That the extra-EU final destination country of the weapon has regularly issued the relative import license or authorization.
- That the Member States or third countries affected by the geographical transit of the cargo have not raised formal security objections or reservations to the ballistic shipment.

To grant the license, pursuant to **Art. 10 of Regulation (EU) 2025/41**, domestic state authorities are bound to take into account international obligations assumed, strategic evaluations made within the CFSP, as well as the subjective qualities of the recipient's honorability and the potential final use of the device, analytically scrutinizing the **risk of diversion of the shipment** with respect to the recipient formally indicated. The mandatory obligation to deny the issuance of licenses is also reiterated if the operation is not in total compliance with comprehensive arms embargoes decreed by the Council of the European Union, the United Nations, or the OSCE, demanding strict prior evaluations to prevent weapons from ending up on black markets or in the hands of terrorist cells.
The reformative intervention of the Parliament and the Council within the **2025-2026** context has further strengthened the administrative control discipline. Priority action has been taken on rules governing the seizure of weapons, ammunition, and essential parts lacking appropriate factory marks or bearing abrase serial numbers, granting national state authorities the power and duty to proceed with their immediate **forced destruction** to permanently remove them from illicit circulation. Furthermore, pending the completion of stamped ballistic marking procedures, weapons imported from extra-EU third countries are subjected to a binding and strict special customs warehouse regime, preventing their premature entry into the civilian market and precluding free movement within the territory of the Union.
The necessity of reinforcing the legal framework governing firearms control was felt at the Euro-unitary level following the dramatic wave of terrorist attacks recorded between 2015 and 2016 (such as the attack on the French satirical newspaper *Charlie Hebdo*, the massacre at the Paris *Bataclan* nightclub, and the coordinated explosions in Brussels on March 22, 2016), theaters where eversive commandos exploited grey market vulnerabilities to equip themselves with ex-ordinance Soviet military assault rifles. With the adoption of the **2015 European Agenda on Security**, the European Commission reaffirmed the strategic centrality of countering illicit arms trafficking within the framework of the fight against transnational crime, intervening to limit civilian access to weapons with higher offensive capability and to hazardous substances usable as precursors for improvised explosive devices (IEDs) or chemical agents.

**FOCUS**

**Civilian Internal Market Control in Directive (EU) 555, 2021**

Faced with the acquisition and lawful possession of weapons by private citizens within the Schengen area, the European regulatory benchmark is **Directive (EU) 2021/555 of the European Parliament and of the Council**, which repealed and entirely replaced the historic Directive 91/477/EEC to gather into a single coordinated text all the technological and ballistic evolutions that occurred over the years. The Directive pursues a delicate institutional balance structured on three pillars:

- **Balancing of Objectives:** It combines the commercial needs of the internal market (relating to the cross-border circulation of civilian firearms for hunting or sporting purposes) with the compelling public safety objectives of the Area of Freedom, Security and Justice.
- **Traceability and Marking:** It mandates that Member States adopt a permanent marking system for all essential components of the weapon (barrel, receiver, slide, bolt) and maintain interconnected digital registries to ensure traceability at any moment.

**Standardization of Civilian Requirements:** It sets minimum subjective requirements (honorability, psychological and physical fitness, absence of criminal records) that private individuals must possess to obtain possession titles or a carrying permit, regulating capillary in Chapter III the cross-border movement of devices within the Union via the prior monitoring of authorities in States affected by transit.

The regulatory framework of the Weapons Directive and its impact on the internal security prerogatives of Member States have been submitted to the scrutiny of legitimacy of the European Court of Justice, which has solemnly secured its validity and *ratio* of protecting public order.

**CASE STUDY**

**Court of Justice of the European Union, Czech Republic v. European Parliament and Council, 2019**

A fundamental jurisprudential pillar for students of the **EU-GLOBACT** module is the historic judgment issued by the **Court of Justice of the European Union on December 3, 2019, in Case *Czech Republic v European Parliament and Council* (C-482/17)**. The Prague Government had filed a partial annulment action against the restrictive amendments introduced by Directive (EU) 2017/853 (subsequently merged into the 2021 text), which had banned civilians from possessing certain high-capacity semi-automatic firearms (weapons derived from military assault rifles), deeming such bans disproportionate and unnecessarily harmful to legitimate trade, collecting, and shooting sports.

The judges of the Court of Justice, rejecting the Czech Republic's appeal in its entirety, clarified the bridging function exercised by European law, establishing three essential dogmatic principles:

**1. The Objective of Constitutional Balance:** The Directive aims to strike a perfect balance between the free circulation of civilian defense products and the compelling guarantees of personal safety and public order, harmonizing national disciplines based on traditionally different approaches (permissive and highly restrictive systems).

**2. The Proportionality of Restrictions:** The limitations and bans imposed on the firepower of semi-automatic weapons do not violate the principle of proportionality and are not unnecessarily harmful to the market, as the primary and eminent goal of the source is safeguarding the public safety of Union citizens against the risk of terrorist massacres or mafia infiltrations.

**3. The Legitimacy of Political Discretion:** The protection of public safety justifies the broad political and economic discretion exercised by the Union legislator under **Art. 114 of the TFEU** (the legal basis of the internal market), legitimizing complex assessments of a social, ballistic, and preventive nature aimed at preventing the hijacking of material toward illicit trafficking channels.

From the systematic analysis of the cited sources, it emerges that the supranational institution, to tackle the phenomenon of illicit arms trafficking, has preferred a strictly administrative approach, regulating capillary the commercial exchange system outward, boundary transit channels, and the regime of industrial transfers within the community territory. As seen in other complex areas of economic crime, a purely central criminal-incrimination approach is absent. However, within certain historical and modern instruments of transnational judicial and police cooperation (former JHA pillar), there is an explicit and constant reference to arms trafficking, manifesting a clear will to extend the effectiveness and operability of such investigative presidios to this specific cross-border penal matter.

Beyond secondary law instruments, the European Union is actively engaged in on-the-field countering through the action of its specialized agencies, most notably those focused on cooperation and forensic analysis, such as **Europol and Eurojust**. The primary purpose of these bodies consists in coordinating in real time the actions of Member States' national judicial authorities (prosecution offices) and police forces, utilizing community tools and databases to strengthen and harmonize counter-measures. The strategic coordination ensured by the Union's agencies allows for much more incisive and effective investigative results against a criminal phenomenon characterized by an immanent transnationality and managed by highly agile private brokers who exploit legislative loopholes and corporate shielding to make public enforcement extraordinarily complex.

Furthermore, contemporary investigative action focuses with particular attention on the scientific study of the correlation and interdependence connecting illicit arms trafficking to other serious illicit trades, with specific reference to human trafficking and *migrant smuggling*.

**FOCUS**

**The Interdisciplinary Approach of the EMPACT Platform**

To dismantle this multi-level criminal convergence, in 2021 the Council of the European Union launched the **EMPACT (European Multidisciplinary Platform Against Criminal Threats)** platform. EMPACT introduces a radically integrated approach at the level of community organs and agencies regarding the protection of internal security, aiming to strengthen and coordinate judicial and police efforts against cross-border crimes. The true strength of this strategic framework lies in its multidisciplinary approach, designed to analyze and sever the interconnections and communicating vessels linking:

- Narcotrafficking flows and human trafficking.
- Clandestine migration smuggling channels and arms contraband.
- Economic, corporate, and fiscal crime circuits.
- The new frontiers of environmental crimes (*green laundering*).
- The transversal impact of *cyber-crimes* and new cryptographic technologies in cyberspace.

Through this integrated and asymmetric operational model, police forces and judiciaries manage to acquire a much more rounded, complete, and penetrating understanding of the actual structural functioning of criminal networks of white-collar professionals and traffickers. This avoids the sterile and inefficient compartmentalization of traditional counter-strategies, offering instead an **holistic, synergistic, and integrated approach** capable of simultaneously attacking the military, logistical, and financial components of criminal cartels, preserving the transparency of the European internal market and securing the Rule of Law.

## X. Key Findings

The dogmatic, historical, regulatory, and jurisprudential analysis carried out within this Art. leads to the delineation of **five fundamental findings** that the student must assimilate for the purpose of passing the exam:

- **Transnational Dimension of the Eurocrime:** Illicit arms trafficking qualifies as a global eversive threat that is structurally cross-border, formally included in the catalogue of **first-tier Eurocrimes pursuant to Art. 83, Paragraph 1 of the TFEU**. The phenomenon moves a financial business volume estimated at billions of dollars a year, feeding on geopolitical crisis areas and porous boundary controls, acting as a profound destabilization factor even within Western States by supplying terrorist cells and mafia networks.
- **The Dual Architecture of the United Nations:** The UN's global strategies are articulated in a speculative manner across two tracks: the **2013 Arms Trade Treaty (ATT)** - a binding treaty centered on the heavy military armament trade between States, which imposes strict prior Risk Assessment obligations under Articles 6 and 7 to ban exports to countries at risk of genocide or violations of *ius cogens* - and the **2001 UN Firearms Protocol supplementing the Palermo Convention**, focused instead on the civilian market between private actors (SALW) and based on the harmonization of the offenses of *illicit manufacturing* and *illicit trafficking*.
- **Tracking Standards and Forensic Marking:** The core of international prevention and *blockchain forensics* rests on the stringent obligations of **permanent marking (stamped serial numbers)** prescribed by Art. 8 of the UN Protocol, joined with the duty of long-term record-keeping and the systems of bilateral import/export authorization under Art. 10. These presidios, combined with the mandatory control and registration of **intermediaries (*brokers*) under Art. 15**, are designed to sever grey market routes and prevent the falsification of cargo documents.
- **The Security Derogation and EU Export Policies:** Although the Euro-unitary legal order is historically bound by the national sovereignty derogation secured under **Art. 346 of the TFEU** (which leaves the protection of essential security interests regarding war material with Member States), the Union intervenes by conditioning external markets through **Common Position 2008/944/CFSP**, which codifies **eight binding guiding criteria** for issuing export licenses of conventional arms to third countries, interfacing with the Dual-Use Regulation.
- **Technological Integration, Internal Market, and the EMPACT Approach:** Modern European reforms - such as **Regulation (EU) 2025/41** (an outbound authorization regime against diversion and *forum shopping*) and **Directive (EU) 2021/555** on the internal civilian market, solemnly secured by the Court of Justice in the **C-482/17 judgment** - coordinate with the need to counter fresh ballistic threats, like reconverted FPV drones and ghost weapons (*Ghost Guns*) printed in 3D. To dismantle the convergence between arms contraband and other Eurocrimes (narcotrafficking, human trafficking, and *cybercrime*), the Union implements the multidisciplinary **EMPACT** platform, replacing old sectoral answers with an holistic, synergistic, and integrated investigative approach between the **Europol and Eurojust** agencies.

# Cybercrime (Computer Crime)

*by Teresa D'Aniello*[*]

SUMMARY: I. What Regulatory Instruments Become Available to The EU Following the Qualification of Cybercrime as A Eurocrime? – II. When does a Simple Digital Action Cross the Boundaries of Legality and become a Cybercrime? – III. How Does the Budapest Convention Align with Domestic Penal Systems? – IV. What Main Categories of Computer Crimes Define Domestic Substantive Law? – V. How Does European Legislation Address Jurisdictional Overlaps in Computer Crimes? – VI. How Does The 2024 UN Convention Innovate the Cybersecurity Framework? – VII. How Are INTERPOL's Modern Global Strategies Structured Against Computer Crime? – VIII. What Function Does Incident Information Sharing Perform Within the Context of European Cybersecurity? – IX. What Is the Impact of The NIS 2 Directive on Critical Infrastructures? – X. How Does the Cyber Solidarity Act Improve European Cybersecurity Policies? – XI. How Does Private Sector Involvement Impact Europol's Digital Threat Prevention? – XII. What Structural Differences Exist Between the US And EU Cyber Regulatory Models? – XIII. How Does the AI Act Regulate Defensive and Offensive Cybersecurity Technologies? – XIV. How Can the Ambiguity of State-Sponsored Cyber-Attack Attribution Be Overcome?

KEY FINDINGS: Cybercrime as a complex and evolving phenomenon; Global regulatory response and the Budapest Convention; Centrality of domestic Italian criminal and procedural protection; The transition toward cyber-resilience and mandatory sharing; Essential involvement of the private sector and security agencies; Protection of digital rights, AI Act, and cyberwarfare frontiers.

## I. What Regulatory Instruments Become Available to The EU Following the Qualification of Cybercrime as A Eurocrime?

Following the qualification of computer crime (*cybercrime*) as a **Eurocrime**, based on **Art. 83, para. 1 of the Treaty on the Functioning of the European Union (TFEU)**, the European Union has acquired a specific criminal competence that allows it to adopt binding regulatory instruments to harmonize the legislations of Member States regarding the definition of offenses and their related sanctions. Art. 83 TFEU constitutes the legal basis that allows the Union to intervene in particularly serious areas of crime that have a cross-border dimension and a high potential for harm, as is the case with cybercrime. The necessity for a common response is dictated by the global nature of these phenomena, which cannot be effectively tackled through isolated national measures.
The **2009 Treaty of Lisbon** formalized the inclusion of cybercrime among the Eurocrimes, recognizing that computer offenses constitute a growing threat to critical

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

infrastructures and public safety. Being phenomena without geographical borders, cybercrime requires international cooperation to be countered effectively.
This qualification is justified by **three main reasons** that we must remember:

- **The cross-border nature of the phenomenon:** It allows cybercrime to be perpetrated from any point in the world and to produce effects across multiple Member States, making purely national actions entirely insufficient.
- **The systemic threat:** It represents a danger to public safety, digital infrastructures, and personal data protection, with potentially devastating impacts on the economy and social stability of the Union.
- **The need for legal uniformity:** The criminal laws of Member States varied significantly, creating severe difficulties in cross-border cooperation and in the uniform enforcement of laws against computer crime. By virtue of this, the European Union has been able to adopt binding regulatory instruments to harmonize national legislations.

**REFERENCES**

**Directive (EU) 40, 2013**
Directive 2013/40/EU of the European Parliament and of the Council represents one of the primary regulatory instruments adopted in implementation of Art. 83, para. 1, TFEU. The latter is expressly cited in the legal basis of the directive, confirming that computer crime is considered one of the particularly serious forms of transnational crime over which the Union has competence to adopt minimum rules of substantive criminal law. The directive, therefore, does not limit itself to establishing obligations for Member States in terms of criminalizing specific conducts (such as illegal access to systems, illegal data interference, use and dissemination of malicious computer tools), but also lays the foundations for a structural strengthening of European cooperation, considering the operational and strategic involvement of supranational agencies such as **Eurojust** and **Europol** (through the European Cybercrime Centre - **EC3**) to be essential.

## II. When does a Simple Digital Action Cross the Boundaries of Legality and become a Cybercrime?

From a technical-legal standpoint, a digital conduct becomes cybercrime when it presents certain essential elements that determine its criminal relevance. First, it requires an active behavior, concretely realized through computer tools, that violates a criminal provision. This conduct must be capable of harming or endangering a protected legal interest – such as system security, data confidentiality, or economic assets – and must be accompanied by the awareness and will to realize it, namely **intent (*dolo*)**. Not every improper use of technology is automatically a crime, but it becomes one when it crosses the threshold of criminal wrongfulness, meaning when the action offends a legally protected interest in a serious and conscious manner.
The boundary between lawful and unlawful, in the computer domain, is rendered particularly blurred not only by the apparent neutrality of digital tools but also by the invisible or automated nature of many conducts. One can consider the simple unauthorized use of a password to access an account: an apparently trivial gesture that, in the presence of intent and an actual or potential harm, can constitute unlawful access with criminal relevance. Or the massive sending of fraudulent emails, which can configure a computer fraud or unlawful data processing.

The purposes pursued by cybercriminals are manifold:

- **Economic advantages:** As in the case of ransomware or digital fraud.
- **Political or ideological goals:** As occurs with hacktivism and attacks on state infrastructures.
- **Personal or relational motives:** As in the more subtle forms of cyberstalking, revenge porn, or coercive control.

In all these cases, digital criminality feeds on the ability to act rapidly, anonymously, and potentially cross-border, escaping classical mechanisms of control and repression. The term cybercrime identifies that set of criminally relevant conducts realized through the unlawful use of information or telecommunication technologies, or that have digital systems, networks, and data as their direct target. It is a criminal phenomenon deeply linked to the digital transformation of society and the growing centrality of information in economic, social, and institutional life.

Computer criminality not only exploits new technologies but develops precisely within the folds of the digital dimension, making the detection of the offense, its repression, and often its definition more difficult. The international legal community has not yet produced a single, universally shared definition of cybercrime, but there is a convergent orientation in recognizing that it encompasses, on the one hand, **proper computer crimes**– namely those aimed at directly hitting the digital infrastructure, such as unauthorized access to a system, data damaging, or interference with a computer system – and, on the other hand, **common crimes committed by means of digital technologies (computer-related crimes)**, such as online fraud, child pornography, or online defamation. In both cases, what characterizes cybercrime is the centrality of the digital environment in the realization of the conduct.

**REFERENCES**

**The Council of Europe Convention on Cybercrime (Budapest Convention), 2001**

At the international level, the first reference regulatory instrument is the **Budapest Convention of 2001**, adopted by the Council of Europe and ratified by numerous States, including non-European ones. The Convention does not provide an abstract definition of the phenomenon but identifies a series of behaviors deemed criminally relevant insofar as they harm the integrity, availability, or confidentiality of computer systems and data. This outlines an open model capable of adapting to continuous technological transformations.

In the European domain, **Directive 2013/40/EU** represented a decisive step for the harmonization of national criminal regulations, introducing a common discipline on main computer crimes and promoting more effective cooperation among Member States. In this context as well, the definition of cybercrime remains functional to the typification of specific behaviors, rather than structured as a general category.

In the Italian context, **Law No. 48 of March 18, 2008** transposed the contents of the Budapest Convention, intervening on the Criminal Code with the introduction and modification of various provisions. Among the most relevant offenses that we must remember are:

- **Unauthorized access to a computer or telecommunication system (Art. 615-*ter* c.c.)**
- **Damaging of computer data, programs, or systems (Art. 635-*bis et seq*. c.c.)**
- **Computer fraud (Art. 640-*ter* c.c.)**
- Offenses related to the use of digital technologies for purposes of sexual exploitation, blackmail, or unlawful dissemination of content.

The classification of cybercrime conducts is divided into two categories:

- **Proper computer crimes**: Conducts directed against hardware, software, or digital data. The goal is to violate the integrity and confidentiality of the system (e.g., DDoS attacks, hacker intrusions, malware dissemination, ransomware).

- **Crimes committed via computers (Computer-related crimes)**: Traditional crimes that find in the network and telecommunication technologies a new and powerful means of execution and dissemination (e.g., telematic fraud, phishing, cyberstalking, online child pornography, defamation on social networks, counterfeiting of non-cash means of payment).

**FOCUS**

**Comparison with other Eurocrimes: The Link between Cybercrime and Terrorism Financing**

Computer criminality increasingly serves as a predicate offense or a logistical operational tool for the commission of other very serious Eurocrimes under Art. 83 TFEU. In international investigative practice coordinated by Europol, a tight link exists with **Transnational Terrorism** and the **Counterfeiting of means of payment**. Terrorist cells exploit cybercrime techniques (such as digital identity theft and phishing) to compromise bank accounts or clone credit cards in order to accumulate clean funds. Furthermore, the proceeds of online fraud and ransomware ransoms are regularly converted into anonymous cryptocurrencies and laundered (connecting to the Eurocrime of **Money Laundering**), providing eversive networks with the financial autonomy necessary to plan attacks or finance online radicalization campaigns without passing through the monitoring of the traditional banking system.

## III. How Does the Budapest Convention Align with Domestic Penal Systems?

The absence of a uniform definitional and sanctioning framework on a planetary level has historically generated deep pockets of impunity, transforming un-updated criminal systems into true legal havens for cybercriminals. The asymmetric and delocalized nature of computer criminality means that a conduct orchestrated on one continent produces systemic damage on another, making the principle of **dual criminality** a potential obstacle to extradition and mutual legal assistance in the absence of harmonized treaties.

**FOCUS**

**The Case of the "ILOVEYOU" Worm, 2000**

The case of the "ILOVEYOU" computer worm, which spread on a global scale in May 2000, highlights in an emblematic way the limits of a fragmented international legal system in the fight against cybercrime. The virus, transmitted via e-mail in the form of an apparently innocent attachment (a fake love message in text format), self-replicated using the user's contact address book and compromised the files present on the device, causing damages estimated at **over 5.5 billion dollars** and hitting strategic world infrastructure and entities such as the CIA, the Pentagon, NASA, and Microsoft.

Investigative computer traces rapidly led to the identification of the suspected author, Onel de Guzmán, a Filipino computer science student. However, the **absence of specific national legislation** regarding computer crimes in the Philippines at the time of the facts prevented any form of domestic criminal prosecution, as well as extradition to the United States of America, precisely due to the **lack of the principle of dual criminality**. This historical episode brought to light how legislative disparities between jurisdictions can offer digital criminals true "safe havens", removing them from the repressive action of States. If a common and binding regulatory framework had existed among the nations involved, based on shared standards and effective judicial cooperation, the sanctioning response would have been far more effective, timely, and symmetrical.

To fill this geo-legal vacuum, the Council of Europe launched the **Budapest Convention of 2001**, which constitutes the first global reference system for the typification of computer crimes and for establishing common procedural rules in digital forensics. The Italian system transposed this multilevel framework through **Law No. 48 of March 18, 2008**, remodeling traditional offenses within the Criminal Code to adapt them to the virtualization of harms.

In order to facilitate university study and mnemonics for the exam, a detailed analysis and comparative study between the international Budapest model and the criminal response of the Italian legislator is presented below:

- **Unauthorized Access**
  - International Model (Art. 2 Convention): Requires intent and the intrinsic unlawfulness of the action. The transnational rule does not consider the presence of a specific unlawful purpose or the material violation of security measures as essential elements for the configuration of the offense.
  - Domestic Italian Discipline (Art. 615-*ter* c.c.): Focuses as a priority on the **violation of security measures** (access keys, credentials, digital barriers) introduced by the owner of the computer space, regardless of the absolute illegitimacy of the access.
  - Main Dogmatic Differences: The Convention does not consider the bypassing of physical or digital security barriers a necessary element, whereas the Italian system does. Furthermore, **unauthorized remaining** in the computer system beyond the limits of the mandate constitutes an autonomous offense in Italy but is not explicit in the Convention.
- **Data Interference**
  - International Model (Art. 4 Convention): Encompasses in an extended and all-inclusive way all intentional conducts of alteration, deletion, deterioration, concealment, or suppression of digital data.
  - Domestic Italian Discipline (Art. 635-*bis et seq*. c.c.): Punishes the damaging of private information, data, and computer programs, but establishes that **criminal prosecution is conditional upon a formal complaint (*querela*) by**

**the injured person**, except in the presence of specific aggravating circumstances (e.g., public assets or strategic infrastructures).
    - Main Dogmatic Differences: In the Italian system, it is necessary for the victim to submit a formal complaint within legal deadlines to activate criminal action (except in cases prosecuted *ex officio*), whereas the international Convention does not provide for this procedural distinction.
- **System Interference**
    - International Model (Art. 5 Convention): Concerns the serious, intentional, and unjustified hindering of the proper functioning of a computer or telecommunication system through the input or damaging of data.
    - Domestic Italian Discipline (Art. 635-*quater* c.c.): Introduces incrimination for the damaging of computer or telecommunication systems. The rule closely mirrors Art. 5 of the Convention, but legal doctrine notes that it was inserted among existing rules in a sometimes confused and stratified manner.
    - Main Dogmatic Differences: The Italian provision represents a direct and literal adaptation of the Convention's article, but it suffers from a partial lack of coordination and clear systematic integration with the traditional structure of the national Criminal Code.
- **Illegal Interception**
    - International Model (Art. 3 Convention): Punishes interception carried out without right, by technical means, of "non-public" transmissions of computer data (from, toward, or within a system). Defines technical means in a partially restrictive manner.
    - Domestic Italian Discipline (Art. 617-*quater* c.c.): Sanctions the illegal interception, prevention, or interruption of computer or telematic communications, but expressly adds liability for the conduct of **revealing or disclosing to the public** the content of the intercepted information.
    - Main Dogmatic Differences: The Italian penal system provides for a severe increase in punishment (special aggravating circumstance) in case of disclosure of protected data and, unlike the Convention, anticipates criminal protection by autonomously punishing the **installation of equipment designed to intercept** under Art. 617-*quinquies* c.c.
- **Computer Fraud**
    - International Model (Art. 8 Convention): Is based on the intentional causing of economic or patrimonial damage to another through any manipulation of data or interference with the functioning of the system. The procurement of an unjust profit is considered merely an element of intent.
    - Domestic Italian Discipline (Art. 640-*ter* c.c.): Configures computer fraud by sanctioning anyone who, by altering the functioning of a system or intervening without right in data, programs, or information, procures for himself or others an **unjust profit with damage to another**.
    - Main Dogmatic Differences: In Italy, the procurement of **unjust profit is an essential constitutive element** of the material fact for the configuration of the offense, whereas in the Budapest Convention it represents exclusively a possible subjective intention of the culprit.

## IV. What Main Categories of Computer Crimes Define Domestic Substantive Law?

**Law No. 547 of December 23, 1993**, entitled "Modifications and integrations to the provisions of the Criminal Code and the Code of Criminal Procedure on the subject of computer crime", marked the **first systematic and organic intervention** of the Italian legislator aimed at adapting the national penal system to the challenges posed by technological evolution and the growing dissemination of criminal phenomena in the digital environment. Prior to this reform, magistrates were forced to apply traditional offenses (such as theft or common damaging) to dematerialized conducts analogously, facing severe constitutional limitations. The reform introduced and typified new criminal offenses within the Criminal Code destined to safeguard the integrity, confidentiality, and security of computer systems and communications.
The main categories of computer crimes introduced by Law 547/1993 that we must remember are:

- **Unauthorized access to a computer or telecommunication system (Art. 615-*ter* c.c.):** Incriminates anyone who enters a computer or telecommunication system protected by security measures without authorization, as well as anyone who remains therein against the express or tacit will of the person entitled.
- **Possession and unlawful dissemination of access codes/damaging programs (Art. 615-*quater* and *quinquies* c.c.):** Punishes the conduct of anyone who, for the purpose of procuring a profit for himself or others or causing damage to others, procures, holds, produces, disseminates, or installs programs designed to compromise, intercept, or interrupt the functioning of computer or telecommunication systems (e.g., dissemination of malware or spyware).
- **Damaging of computer or telecommunication systems (Art. 635-*bis* c.c.):** Provides a specific hypothesis of damaging aimed at hitting the efficiency, integrity, and functionality of electronic systems, data, and programs, safeguarding public and private interests in the availability of digital services.
- **Illegal interception, prevention, or interruption of computer or telecommunication communications (Art. 617-quater c.c.):** Disciplines and punishes conducts harming the freedom and secrecy of communications carried out via computer or telecommunication means, equalizing virtual space to the private domicile.
- **Computer fraud (Art. 640-*ter* c.c.):** Punishes anyone who, by altering in any way the functioning of a computer or telecommunication system or intervening without right in any modality on data, information, or programs, procures for himself or others an unjust profit with damage to another, configuring a technologically evolved form of the crime of swindling.

The repressive system introduced by Law 547/1993 constituted the foundation of criminal discipline in the field of computer crime, subsequently integrated and updated by **Law No. 48 of March 18, 2008**, with which Italy ratified and executed the **Council of Europe Convention on Cybercrime (Budapest, 2001)**. The latter introduced further reforms on both substantive and procedural levels, strengthening the regulatory response to computer crimes and promoting more effective international judicial cooperation instruments.

**REFERENCES**

**Italian Code of Criminal Procedure, Art. 51, 3-*quinquies***

One of the innovations of greatest relief introduced into the Italian procedural system with the transposition of the Budapest Convention via Law No. 48 of 2008 concerns the modification of Art. 51 of the code of criminal procedure, with the insertion of para. 3-*quinquies*. The provision attributes **exclusive functional competence in the matter of computer crimes** (including Articles 615-*ter*, 617-*quater*, 635-*bis*, and 640-*ter* c.c.) to the public prosecutor at the Court of the capital of the district of the Court of Appeal, establishing the so-called **District Prosecutor's Office for Computer Crimes**.

**FOCUS**

**The *Ratio* of Judicial Centralization**

This regulatory choice of the Italian legislator responds to the technical and investigative necessity of tackling in a coordinated manner criminal phenomena characterized by a strong transnational dimension, the immateriality of evidence, and the structural difficulty of identifying a territorial scope or a *locus commissi delicti* of reference, as typically occurs in cybercrimes. The centralization of investigations at District Prosecutor's Offices allows:

- Greater immediate coordination between national and international investigative authorities (through the channels of **Europol and Eurojust**).
- The development of a high **technical and computer-forensic specialization** by the magistrates and judicial police units in charge (Postal and Communications Police).
- A homogeneous and swift judicial response, suitable to overcome territorial jurisdictional conflicts linked to the fluid nature of telecommunication networks.

The historical evolution of computer criminal law in Italy has followed three major steps:

- **Pre-1993 Phase (Regulatory Vacuum):** Absence of specific offenses; judges apply common offenses (e.g., swindling or damaging of movable things), clashing with the prohibition of analogy *in malam partem*.
- **National Typification Phase (Law 547/1993):** Introduction of proper offenses (Articles 615-*ter*, 640-*ter* c.c.); protection of "computer space" as an autonomous legal interest.
- **International Harmonization Phase (Law 48/2008 - Budapest):** District centralization of investigations (Art. 51 c.c.p.); introduction of sanctions for the administrative liability of entities (Legislative Decree No. 231/2001) for computer crimes and hardening of penalties for attacks on critical infrastructures, in line with **Directive 2013/40/EU**.

## V. How Does European Legislation Address Jurisdictional Overlaps in Computer Crimes?

The growing dissemination of computer criminality at a transnational level has challenged traditional criteria for attributing criminal jurisdiction, based on the principle of territoriality, according to which the State exercises its judicial authority in relation to crimes committed within its geographical borders. Cyberspace, by its nature, is devoid of physical boundaries, making the application of traditional concepts of *locus commissi delicti* inadequate. In response to this complexity, European law has sought to address the critical issues connected to the overlap of investigations and jurisdictional fragmentation through the introduction of regulatory instruments aimed at guaranteeing effective judicial and investigative cooperation among Member States.

One of the first regulatory interventions in this sense is represented by **Council Framework Decision 2005/222/JHA** on attacks against information systems. Inspired by the Budapest Convention, it constituted the first binding regulatory act at the European level in the field of computer criminality. An innovative aspect introduced by the Decision concerns the provision of criteria for resolving conflicts of jurisdiction, which can arise when multiple Member States claim competence to prosecute criminally for the same criminal fact. The ultimate purpose of these provisions is to favor a rational distribution of jurisdictional competences, avoiding the risk of multiplication of criminal proceedings, negative conflicts of competence (namely investigative inertia due to jurisdictional uncertainty), or phenomena of criminal forum shopping, as well as guaranteeing operational coordination between competent authorities, also through judicial cooperation instruments and recourse to specialized European bodies, such as **Eurojust**.
This Framework Decision was subsequently succeeded by **Directive 2013/40/EU**, which repealed its provisions, offering a more organic and detailed regulatory framework. The Directive, in addition to typifying with greater clarity criminal offenses related to attacks against information systems – such as unauthorized access, illegal data interference, and the use of computer tools for the commission of offenses – strengthened the principle of operational cooperation among national authorities, both in the investigative phase and in the trial phase, fixing rigid cross-border jurisdictional criteria that bind Member States.

**REFERENCES**

**Directive (EU) 40, 2013, Art. 12**

"1. Member States shall establish their jurisdiction with regard to the offenses referred to in Articles 3 to 8 where the offense has been committed: a) in whole or in part on their territory; or b) by one of their nationals, at least in cases where the act constitutes a criminal offense at the place where it was committed.
2. When establishing their jurisdiction in accordance with paragraph 1, letter a), a Member State shall ensure that it has jurisdiction where: a) the offender commits the offense when physically present on its territory, whether or not the offense is against an information system on its territory; or b) the offense is against an information system on its territory, whether or not the offender was physically present on its territory at the time of committing the offense.
3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offense referred to in Articles 3 to 8 committed outside its territory, including where: a) the offender has his or her habitual residence in its territory; or b) the offense is committed for the benefit of a legal person established in its territory."

To understand the effective extension of the protection of "virtual space" and the application of these jurisdictional criteria, we must consider how the domestic Italian system qualifies the material object of the conduct, namely the very notion of a computer system, overcoming old physical limits.

**CASE STUDY**

**Italian Cassation Court, Fifth Penal Section, No. 40470, 2018**

The Court of Cassation, in judgment No. 40470 of 2018, affirmed a principle of fundamental systematic relief in the matter of computer crimes, clarifying that the notion of **"computer system"** cannot be reduced solely to the presence of a connection or an interconnection in a network, but must be understood in a broad and substantial sense. According to the Supreme Court, what matters for the purposes of criminal protection (e.g., for the application of Art. 615-*ter* c.c.) is the **aptitude of the machine (hardware) to organize and process data**, based on a program (software), for the pursuit of heterogenous purposes. Beside the function of mere registration and storage of data, the activity of processing and organizing the data themselves must also be present.

The judges of legitimacy specified that it appears completely **irrelevant that the apparatus is not connected to a telecommunication network**, provided that it is structured to operate according to logics proper to computer science (offline systems). The Court clarifies that internal criminal law has not provided a rigid regulatory definition of a computer system, but that, in the absence of a legislative classification, it is the case law of legitimacy that must specify its contours, in light of the **protective function of the "*ius excludendi alios*"** that the rule intends to pursue. This orientation strengthens the idea that protection extends to all those devices whose structure allows even partially the use of digital technologies (e.g., electronic safes, automotive control units, evolved cash registers) and imposes a substantial evaluation of the device's characteristics, based on its real operational functionalities and not on its mere formal classification.

The criteria for attributing jurisdiction in cybercrimes *ex* art. 12 of Directive 2013/40/EU are:

- **Criterion of Physical Presence (Offender):** The Member State is competent if the hacker or cybercriminal carried out the telematic action while physically located on its territory, regardless of nationality or the location where the targeted server is situated.
- **Criterion of the Targeted Infrastructure (Target):** The Member State holds jurisdiction if the computer system or the server victim of the attack is located on its geographical territory, even if the perpetrator acted physically from a third or non-EU State.
- **Criterion of Nationality and Habitual Residence:** Active competence for computer crimes committed abroad by its own nationals (subject to dual criminality) or by individuals stably residing in the territory of the State.
- **Criterion of Corporate Benefit (Legal Person):** Extension of the Member State's jurisdiction where the transnational cyber-attack was perpetrated to procure an economic or strategic advantage for a company or legal person that has its registered office in the territory of the State (connecting with the **Liability of Entities under Decree 231/2001**).

## VI. How Does The 2024 UN Convention Innovate the Cybersecurity Framework?

The **2024 United Nations Convention on Cybercrime** represents a regulatory evolution of historical scope compared to the 2001 Budapest Convention, redefining the architecture of judicial and police cooperation on a planetary level. While the Budapest framework was born within the Council of Europe – configuring itself as a regional treaty open to the accession of third countries – the new UN Convention rests on an **ambition**

**of multilevel universality**, addressing technological asymmetries between the Global North and South.

The innovativeness of the United Nations text is based on **four strategic aspects** that we must keep in mind:

- **Inclusive Global Participation:** The text overcomes Western geopolitical blocs by extensively involving **developing countries**. Broadening the baseline of participation aims to clear out digital "safe havens", harmonizing the criminal response even in those jurisdictions that historically lacked resources to update their codes.
- **Cross-Border Common Penal Policy:** The UN Convention pursues, as a priority, a common penal policy aimed at protecting society from computer crime. This objective is enacted through the typification of new offenses and common procedural powers that take into account the total virtualization of economic assets and data.
- **Obligation of Technical Assistance and Capacity Building:** Unlike previous treaties, the UN introduces a true pillar of **solidary cooperation**. Technologically advanced States have an obligation to provide forensic software, training, and structural support to countries with lower operational capacity, strengthening the global resilience of networks and the stability of digital forensics systems.
- **Institutionalization of INTERPOL's Role:** The text recognizes and codifies the essential role of **INTERPOL**, the international criminal police organization that reunites 196 States. INTERPOL is integrated as the primary nerve hub to facilitate the **rapid, secure, and encrypted exchange of information** and digital evidence among the investigative authorities of different continents.

**REFERENCES**

**United Nations Convention against Cybercrime, 2024, Preamble and Purposes**
The Convention establishes that States Parties undertake to promote and strengthen measures aimed at preventing and combating computer crime more efficiently and effectively, promoting, facilitating, and supporting international cooperation and technical assistance, including the development of technological capabilities of police forces, in full respect of the rule of law and human rights.

The 2024 UN Convention dedicates wide space to the intersection between information and communication technologies (ICT) and the most serious forms of transnational organized crime. In international application practice, an indissoluble link emerges between cybercrime and the Eurocrime of **Trafficking in human beings**. Modern criminal networks use computer techniques not only for the digital recruitment of victims (e-recruitment) but exploit the black markets of the Darknet to purchase surveillance and geolocalized tracking software for exploited migrants. Furthermore, large-scale computer frauds and banking system breaches managed by hacker cells serve to produce the liquidity necessary to finance the logistics and transport of victims across the borders of the European Union, highlighting how computer crime is by now the enabling infrastructure of all other Eurocrimes under Art. 83 TFEU.

**FOCUS**

**Comparative Study of Conventions on Cybercrime (Budapest 2001 v. UN 2024)**

**Budapest Convention (2001 - Council of Europe):**

- Genesis: Euro-Atlantic and regional matrix.
- Focus: Typification of classical computer crimes (unauthorized access, data interference).
- Limits: Difficult penetration in developing countries due to the lack of structured financial and technical assistance tools.

**UN Convention on Cybercrime (2024):**

- Genesis: Universal matrix (United Nations General Assembly).
- Focus: Multidisciplinary approach to ICT, countering the illicit use of cryptocurrencies, and timely removal of terrorist and child pornography content.
- Innovation: Obligation of international Capacity Building, 24/7 emergency cooperation, and a direct portal through the INTERPOL network.

## VII. How Are INTERPOL's Modern Global Strategies Structured Against Computer Crime?

The study of computer crime and its relative defense strategies demands an in-depth analysis of its historical origins. This analysis demonstrates that the birth of modern **cybersecurity** was not the result of theoretical planning, but rather an immediate reaction to large-scale computer incidents that exposed the intrinsic fragility of early global network infrastructures.

**FOCUS**

**The "Morris Worm" and the Birth of Cybersecurity, 1988**

The **Morris Worm** was one of the most significant and disruptive events in the history of information security, marking the **first major large-scale attack on the Internet**. Released on November 2, 1988, the worm was designed and launched by Robert Tappan Morris, a graduate computer science student at *Cornell University*. The original intent, according to the defense, was purely exploratory – aimed at measuring the size of the Arpanet network (the ancestor of the Internet). However, due to a programming error in the code, the worm began to replicate uncontrollably. The algorithm rapidly infected thousands of computers connected to the network, overloading processors, causing system crashes, total service disruptions, and considerable economic and logistical damage to universities, research centers, and US military laboratories.

Under the profile of judicial prosecution and comparative criminal law, Morris was indicted under the **Computer Fraud and Abuse Act (CFAA) of 1986**, historically becoming the **first individual convicted** under this special legislation on computer crimes in the United States of America. In 1991, the federal Court sentenced him to three years of probation, a $10,050 fine, and mandatory 400 hours of community service.

The Morris Worm represented a radical **turning point in the history of information security**, drastically increasing the awareness of public and private institutions regarding structural network vulnerabilities and the risks connected to malware codes capable of self-replicating autonomously. The incident highlighted how exposed and defenseless systems were against new types of asymmetric attacks. One of the most significant institutional and procedural consequences of the event was the immediate creation of the first **Computer Emergency Response Team (CERT)**, a technical rapid-response body tasked with providing support, analysis, and central coordination during computer emergencies. The attack also pushed the scientific community to develop and deploy the first essential tools for advanced perimeter defense, such as **firewalls** and network intrusion detection systems (IDS), paving the way for modern cybersecurity. The Morris Worm case established itself as a crucial jurisprudential precedent, proving the urgent need for specific criminal regulations and security structures ready to respond to digital threats.

Having outlined the historical origins of the phenomenon, in the current technological and geopolitical scenario of **2026**, governance and the global operational response to advanced cybercrimes are entrusted to the coordination of INTERPOL, which implements multi-year action plans to support the law enforcement forces of its 196 Member Countries.

The INTERPOL Strategic Framework 2022-2025 is the multi-year planning instrument through which the Organization defines its operational, institutional, and technological priorities to strengthen the support provided to national law enforcement. Approved by the General Assembly at its 89th session (November 2021), the document adopts a global, future-oriented approach to address the emerging challenges of transnational and computer crime. The programmatic plan is articulated across **four strategic objectives** and 17 operational targets that we must remember:

- **Trusted information for action:** The aim is to thoroughly strengthen access to and interoperability of INTERPOL's information systems and databases by national police authorities, guaranteeing the secure use of data and the development of high-quality criminal and forensic analyses. Strict and binding compliance with international standards on personal data protection and fundamental rights is central and mandatory, serving as an indispensable element to consolidate mutual trust among States using the Organization's protected communication systems.

- **Partnerships for global security:** INTERPOL aims to consolidate its role as the central global platform for immediate information exchange and operational coordination in the fight against transnational organized crime. This strategic objective includes promoting diversified partnerships with the private sector (tech companies), strengthening the technical capabilities of Member States (particularly developing countries through dedicated programs), and actively contributing to United Nations regulatory processes by offering strategic recommendations in the fight against advanced computer crime, in perfect synergy with the new 2024 UN Convention.
- **Innovation in policing (Smart Policing):** Through a massive push toward digitalization and the native integration of emerging technologies (such as Artificial Intelligence applied to predictive policing and data analytics software), INTERPOL intends to improve the efficiency of its investigative processes and the quality of services offered to Member Countries. In this perspective, promoting a permanent global dialogue with public and private actors is vital to developing innovative forensic solutions to counter crime.
- **Organizational efficiency and governance:** Strengthening the Organization's operational and administrative capacity requires modern leadership, decentralized resource management, and an internal corporate culture strictly grounded in the values of ethics, total transparency, and inclusion. Particular attention is dedicated to organizational resilience in the face of geopolitical crises, integrated risk management, and the consolidation of the internal legal framework to secure the institution.

## VIII. What Function Does Incident Information Sharing Perform Within the Context of European Cybersecurity?

The sharing of incident information performs a **strategic and advanced prevention function** within European cybersecurity, configuring itself as an essential tool to guarantee systemic resilience, operational continuity of the single market, and a coordinated response capacity against asymmetric transnational threats. Cyberspace renders obsolete old models of isolated defense: a ransomware or DDoS attack hitting an infrastructure in one Member State represents an immediate alarm bell for the entire Union.

The architecture of community cybersecurity has historically structured itself through **Regulation (EU) No 526/2013**, which imposed on Member States the obligation to designate competent national authorities and to establish **CSIRTs (Computer Security Incident Response Teams)**, with the aim of creating an integrated, synergistic network to mitigate threats beyond geographical borders. This obligation, formalized through provisions requiring the mutual exchange of information regarding significant digital incidents, configures itself as an indispensable mechanism for timely monitoring and coordinated crisis management, strengthening the collective protection of the Union. The community regulatory action provides for information regarding incidents to be shared in a structured, standardized, and continuous manner between designated national authorities, allowing for the alignment of operational responses on the field and guaranteeing effective emergency management. Within this multilevel ecosystem, **ENISA (The European Union Agency for Cybersecurity)** plays a central role, acting

as a coordination hub and facilitating the transfer of knowledge, predictive analyses, and best practices among Member Countries.

The regulatory framework on information security at the community level was subsequently consolidated and standardized through the **Cybersecurity Act (Regulation EU 2019/881)**, which repealed and replaced the previous Regulation 526/2013, granting ENISA a **permanent mandate** and equipping it with greater resources. This regulatory pillar introduced, among other structural measures, the first **European cybersecurity certification framework** for ICT products, processes, and services. This system aims to standardize and elevate the security level of digital devices placed on the market (from corporate software to Internet of Things – IoT – devices), guaranteeing adequate protection against the growing technological sophistication of attacks. The Cybersecurity Act also establishes and values the **Interinstitutional Cybersecurity Board (IICB)**, a special body tasked with monitoring, supporting, and supervising the implementation of cybersecurity measures specifically within European Union institutions, bodies, and agencies, favoring constant dialogue with national authorities and supporting the development of common guidelines.

In the current context of **2026**, this framework for sharing information and the resilience of critical infrastructures has found its definitive operational fulfillment through the mandatory transposition of the **NIS 2 Directive (Directive EU 2022/2555)**. This text has drastically raised security standards for essential sectors (energy, transport, banking, health, and digital infrastructures), introducing a strict obligation for **early warning notifications of significant incidents within 24 hours** to the national authority and ENISA, backed by severe administrative and financial sanctions for non-compliant corporate executives.

**REFERENCES**

**Regulation (EU) 881, 2019, Art. 4**

The Regulation establishes that ENISA shall pursue the objective of achieving a high common level of cybersecurity across the Union, supporting Member States and European institutions in developing operational capabilities and cross-border cooperation, promoting the timely sharing of information on cyber threats and incidents among all strategic network actors.

**FOCUS**

**Eurocrime Interconnection: Computer Fraud and the Counterfeiting of Non-Cash Means of Payment**

The rapid sharing of information on computer incidents coordinated by ENISA and Europol proves to be an essential safeguard to restrict the ramifications of other Eurocrimes under Art. 83 TFEU. There is a direct operational link with the **Counterfeiting of non-cash means of payment** (protected by Directive EU 2019/713). When a structured criminal group launches an advanced cyber-attack against an EU banking institution's home banking system or inoculates a malware into commercial POS terminals, the event is classified as a cybersecurity incident. The immediate sharing of technical data and "Indicators of Compromise" (IoCs) through the European CSIRT network allows other banks and Eurozone supervisory authorities to proactively shield their servers. This blocks mass credit card cloning, financial identity theft, and subsequent telematic fraud, stopping the laundering of illicit capital at its source.

The European Architecture for Cyber Incident Sharing and Management is divided into four phases:

- **Phase 1 - Detection and Early Warning (National/Corporate Level):** An operator of essential services (e.g., a hospital or power plant) suffers a cyber-attack and is obliged under the NIS 2 Directive to submit an early warning notification within 24 hours to the competent national CSIRT.
- **Phase 2 - Centralization and Forensic Analysis (ENISA):** The national CSIRT transfers the technical data to ENISA. The agency analyzes the malware, isolates its digital signature, and drafts a technical risk mitigation report.
- **Phase 3 - Cross-Border Dissemination (CSIRTs Network):** ENISA distributes the security alert to all CSIRTs across the other 26 Member States, enabling proactive blocking of servers and communication ports on a continental scale.
- **Phase 4 - Internal Institutional Monitoring (IICB):** The IICB applies the same security standards within the servers of the European Parliament, Commission, and Council, verifying the defense and impermeability of the Union's own systems against external threats.

## IX. What Is the Impact of The NIS 2 Directive on Critical Infrastructures?

The adoption of **Directive (EU) 2022/2555 (known as the NIS 2 Directive)** has significantly impacted the European system for protecting critical infrastructures, moving past the limitations inherent in the previous Directive (EU) 2016/1148 (NIS 1) and radically strengthening the regulatory framework of cybersecurity.

NIS 1 represented the first historic step toward harmonized regulation at the European level regarding the security of network and information systems. It introduced minimum obligations for **Operators of Essential Services (OES)**, active in strategic fields such as energy, transport, healthcare, and finance, as well as for **Digital Service Providers (DSPs)**. Central to this was the provision of a cooperation mechanism between Member States via **CSIRTs** and the NIS Cooperation Group, aiming to strengthen the collective response to cyber incidents.

However, concrete enforcement experience highlighted significant structural weaknesses in NIS 1: fragmented and inconsistent approaches among Member States (due to excessively wide margins of discretion in national transposition), limited subjective scopes of application, an absence of common security criteria, and a lack of incisiveness in criminal and administrative sanctions. With NIS 2, the European Union intervened to build a more coherent, comprehensive, and resilient system, adapted to the new technological and geopolitical context of **2026**.

Compared to NIS 1, the new directive does not merely update but **redefines the entire regulatory architecture**, focusing on four macro-innovations that we must remember:

- **Removal of the OES/DSP Distinction and Subjective Expansion:** The old classification between operators of essential services and digital service providers has been eliminated, replaced by size-based criteria establishing two new categories: **"Essential Entities"** and **"Important Entities"**. This expansion includes public administrations, manufacturing sectors, chemicals, waste management, and postal services.
- **Supply Chain Security:** Increased attention is directed toward the security of commercial and technical relationships with external ICT partners and vendors, identified by ENISA as potential systemic **single points of failure**.

- **Direct Governance Accountability:** Specific obligations are introduced that directly involve **management bodies and board members** of the affected organizations. They face personal liability, including financial penalties, for failing to approve or supervise corporate cyber risk management measures.
- **Harmonized and Effective Sanctioning Regime:** It introduces administrative and statutory fines aligned with the GDPR model, providing for financial penalties of up to **10 million euros or 2% of the total worldwide annual turnover** for non-compliant essential entities.

**REFERENCES**

**Directive (EU) 2555, 2022, Art. 21**

Art. 21 mandates that essential and important entities take appropriate and proportionate technical, operational, and organizational measures to manage risks posed to the security of network and information systems. These measures must strictly include: risk analysis policies, incident handling, business continuity (business continuity and disaster recovery), supply chain security, cryptography, and the use of multi-factor authentication (MFA) solutions.

The structural differences between the NIS 1 and the NIS 2 Directive are the following:

- **Subjective and Objective Scope of Application**
  - NIS 1 Directive: Restricted to predefined traditional essential sectors such as energy, transport, health, and banking, leaving wide margins of discretion to States in identifying individual operators.
  - NIS 2 Directive: Extended to a wide range of strategic sectors, including digital services, cloud computing providers, e-commerce portals, electronic communication networks, and all critical and important infrastructure providers based on clear size thresholds.
- **Cyber Risk Management Obligation**
  - NIS 1 Directive: Provided a general, generic, and abstract obligation to adopt proportionate security measures for networks and information systems.
  - NIS 2 Directive: Introduces a strict focus on technical risk management, mandating specific security measures and an absolute obligation to control and audit **supply chain security**.
- **Timeframes for Incident Reporting and Notification**
  - NIS 1 Directive: Stated that a serious incident had to be reported to competent national authorities or CSIRTs without undue delay, a parameter typically quantified as within **72 hours**.
  - NIS 2 Directive: Drastically tightens reaction times, mandating that a significant incident must be reported via an initial early warning alert **within 24 hours** of becoming aware of it.
- **Sanctioning and Liability Regime**
  - NIS 1 Directive: Provided for sanctions in case of non-compliance, but these were less severe, lacked common statutory maximums, and were fragmented among individual national legislators.
  - NIS 2 Directive: Introduces much more severe, harmonized penalties based on the GDPR model, including hefty administrative-financial fines proportional to global turnover and personal civil liability for board members.
- **Cooperation and Information Exchange Between Member States**

  - NIS 1 Directive: Regulated limited cooperation and a primarily formal or voluntary coordination between different national authorities.
  - NIS 2 Directive: Mandates a radical reinforcement of mandatory cross-border cooperation, featuring active, standardized, and real-time exchange of information on cyber threats and emerging software vulnerabilities.
- **Powers of Competent National Authorities**
  - NIS 1 Directive: Established that each Member State should designate one or more responsible authorities, which were often devoid of real powers for direct inspections or corporate audits.
  - NIS 2 Directive: Requires every Member State to have centralized cybersecurity authorities that are structurally stronger and armed with **greater powers of proactive oversight, criminal, and administrative enforcement**.
- **Protection and Resilience of Critical Infrastructures**
  - NIS 1 Directive: Regulated the protection of critical infrastructures at the community level, but in a less detailed manner that lacked a synergistic link with physical security.
  - NIS 2 Directive: Places major strategic emphasis on coordinated **global resilience and protection**, working in tandem with the CER Directive (EU 2022/2557) on the physical resilience of critical entities.

## X. How Does the Cyber Solidarity Act Improve European Cybersecurity Policies?

The **Cyber Solidarity Act**, formally approved by the European Union and entering fully into force in **February 2025**, represents the operational pillar of European collective cyber defense. This regulation introduces a complex set of legal, financial, and operational measures aimed at overcoming the fragmented defensive approaches of individual Member States, establishing instruments designed to strengthen capabilities to prevent, detect, and handle cyber threats with cross-border or potentially systemic impacts.
The architecture of the regulation rests on **four operational pillars** that we must keep in mind:

- **The European Cyber Shield:** An integrated, cross-border network of **national and multi-state Security Operation Centres (SOCs)**. These centers, utilizing advanced artificial intelligence and data analytics, are tasked with continuous network traffic monitoring, immediate technical information sharing on emerging threats, and defining coordinated Union-wide responses.
- **The EU Cybersecurity Reserve:** A genuine "task force" consisting of **highly specialized and accredited private security and emergency response services**. These vendors are deployable and financially covered by EU funds to offer immediate emergency interventions in the event of severe cyber-attacks against public institutions or critical infrastructures, guaranteeing rapid, structured operational support.
- **The Cyber Incident Review Mechanism:** A review process for significant incidents through which the dynamics, exploited vulnerabilities, and consequences of major attacks are analyzed. The goal is to draw lessons from systemic failures to update the Union's preventive strategies and increase operator accountability.

- **Regular Testing of Vulnerable Sectors:** Funding and planning systematic security audits of information systems in the most exposed compartments (energy, finance, transport, and healthcare) to detect structural weaknesses before threats can materialize on the field.

**REFERENCES**

**Regulation (EU) 38, 2025, General Objectives**
The legislative text establishes a Union solidarity mechanism to strengthen common detection capabilities and situational awareness of cyber threats. It sets up a cybersecurity reserve at the European level to assist Member States in the event of significant or large-scale incidents, ensuring single market continuity and internal security.

The solidarity measures and the Cyber Shield established by the Cyber Solidarity Act have become essential in the current **2026** geopolitical context to counter connections between cybercrime and other Eurocrimes under Art. 83 TFEU, particularly **Transnational organized crime**. Modern criminal syndicates and state-sponsored hacker groups coordinate cyber-attacks on port logistics or customs systems, not merely for extortion, but to temporarily paralyze security checks. The European shield of SOCs allows for the interception of these anomalous intrusions in real time, preventing system lockouts from being exploited as a diversion to facilitate the smuggling of illicit shipments connected to **Drug trafficking** or **Human trafficking**.

**FOCUS**

**Technological Evolutions: The Quantum Security Transformation, 2025**
Throughout **2025** and **2026**, the field of cybersecurity is experiencing a radical transformation driven by the adoption of quantum technologies and the definition of new digital sovereignty models for the Union. This scenario, constantly monitored by ENISA and national authorities, articulates around three technological and legal pathways:

- **Post-Quantum Cryptography (PQC):** Emerging as the mandatory foundation to protect the Union's strategic communications against decryption threats posed by future quantum computers, utilizing complex mathematical algorithms that ensure unbreakable security.
- **Quantum Key Distribution (QKD):** Advanced protocols based on quantum physics that make it virtually impossible to intercept or spy on the exchange of encryption keys, since any interception attempt alters the physical state of the particles, immediately alerting the system.
- **Predictive Models and Adaptive Defenses:** Risk assessment in critical infrastructures evolves by integrating technical tools of quantum artificial intelligence to anticipate threats and react flexibly, establishing criteria for shared responsibility and operational transparency between public and private actors.

## XI. How Does Private Sector Involvement Impact Europol's Digital Threat Prevention?

In a geopolitical and technological context characterized by increasingly sophisticated, rapid, and transnational cyber threats, public-private cooperation is no longer an optional accessory, but rather a **structural necessity** to guarantee the effectiveness of the Union's cybersecurity policies and criminal law enforcement. **Europol** (the European Union Agency for Law Enforcement Cooperation) has progressively extended its mandate in

response to the digitalization of criminal activities. This institutional evolution saw a fundamental turning point with the establishment and reinforcement of the **European Cybercrime Centre (EC3)**, a highly specialized structure operating within the agency to coordinate the EU's strategic and operational response to computer crime.
The EC3 exercises its competence in computer crime by focusing on **three macro-areas of high social alarm** that we must remember:

- **Cybercrimes for profit:** Conducts managed by transnational organized crime groups aimed at producing massive illicit financial flows, such as e-commerce fraud, large-scale phishing, and ransomware attacks targeting banking institutions.
- **Cybercrimes causing serious harm:** Computer crimes directly attacking human dignity and fundamental rights, with specific reference to online child sexual exploitation and abuse (CSAM - Child Sexual Abuse Material).
- **Attacks against critical infrastructures:** Structured actions directed against information systems of strategic importance for Member States (e.g., Distributed Denial of Service – DDoS attacks against energy or health networks), aimed at paralyzing essential services.

In this framework, strategic collaboration with the private sector assumes a crucial role. Private enterprises – particularly major technology companies (Big Tech), Internet Service Providers (ISPs), cybersecurity firms, and financial institutions – are structurally the first actors to have immediate visibility over new software vulnerabilities and anomalous network traffic flows.
Their active involvement allows for a **two-way flow of information**: on one side, Europol and the EC3 benefit from timely data, advanced technical expertise, and cutting-edge forensic technologies; on the other, private companies receive directives, Indicators of Compromise (IoCs), and institutional support to prevent the escalation of threats and protect their customers. Through the EC3, Europol has institutionalized this synergy through structured partnerships aimed at exchanging operational intelligence, sharing digital investigative tools, and co-developing advanced cyber-defense technologies, raising the cyber-resilience of the European Space.

**FOCUS**

**Investigative Practice: The EC3 Strategic Tools (The IOCTA Report and the J-Cat)**
To guide the field activities of law enforcement forces and define the action priorities of the permanent **EMPACT** platform, the European Cybercrime Centre relies on two strategic operational instruments:

- **The IOCTA Report (Internet Organised Crime Threat Assessment):** An in-depth assessment that the EC3 drafts and publishes periodically. This document provides quantitative operational data, strategic intelligence, and analyses of emerging trends in cybercrime (e.g., the abuse of artificial intelligence for hostile attacks or the evolution of cryptocurrency scams), serving as a compass for European legislators and investigators.
- **The J-CAT (Joint Cybercrime Action Taskforce):** A permanent operational taskforce hosted at the headquarters of the EC3. The mission of the J-CAT is to coordinate and execute complex cross-border investigations and operations based on intelligence, aimed at countering and dismantling the primary networks of hackers and digital criminals, drawing on direct operational support from liaison officers seconded from Member Countries and international partners (e.g., the United States, United Kingdom).

## XII. What Structural Differences Exist Between the US And EU Cyber Regulatory Models?

The phenomenon of cybercrime is not limited to the mere alteration of network systems, but qualifies as an asymmetric eversive tool aimed at the **exfiltration and commercialization of private, corporate, and strategic information assets**. Personal and industrial data constitute the true currency of exchange in the digital economy, turning storage servers into the primary target of targeted attacks managed by transnational cartels.

**FOCUS**

**Crimes on Information assets (Sony Pictures 2014 & Equifax 2017)**

The analysis of international practice highlights two landmark cases that illustrate the differing nature of digital offenses:

- **The attack on Sony Pictures (2014):** Represents the prototype of corporate cyber-sabotage with a geopolitical matrix. Structured hacker cells breached the multinational's servers, exfiltrating and disseminating online confidential executive emails, unreleased scripts, and protected financial data. The event caused not only devastating direct economic damage, but a **severe, permanent impact on commercial reputation** and the security of intellectual property, highlighting the vulnerability of digitalized industrial secrets.
- **The Equifax system breach (2017):** Constitutes one of the most severe and massive data breach cases in global economic history, operating as a direct attack on consumers. Cybercriminals exploited a known, unpatched *software* vulnerability to penetrate the databases of one of the main credit reporting agencies in the US. The attack **exposed the personal and sensitive data of over 140 million individuals**, including social security numbers, dates of birth, driver's licenses, and protected financial details, putting the privacy and economic security of a massive segment of the population at risk and fueling the Eurocrime of **Counterfeiting of non-cash means of payment** through subsequent financial identity theft.

Under the profile of comparative law, the Equifax case highlighted the structural weaknesses of the **United States data protection system**. The regulatory approach of the United States relies on a **sectoral, fragmented, and inconsistent framework** (*patchwork approach*), devoid of an omnibus federal privacy law, which leaves wide regulatory gaps and creates asymmetries of protection across different States.
Conversely, the European Union adopted an opposing regulatory philosophy based on the precautionary principle and the centrality of an individual's fundamental rights. Through the **GDPR (Regulation EU 2016/679)**, the Union imposed a **comprehensive, uniform, and directly applicable model** across the EU, built on the principles of *privacy by design* and *accountability*. This framework mandates *data breach* notifications within 72 hours and levies severe sanctions proportional to a company's global turnover. This rigorous protective architecture applies not only against external illicit intrusions, but serves as a preventive and sanctioning shield against emerging technologies and commercial artificial intelligence systems.

**FOCUS**

**The Italian *Garante della Privacy*'s Injunction on ChatGPT, 2023**

Particularly significant regarding future developments, including criminal ones (connected to large-scale illicit data processing), is the decision taken via **Injunction No. 112 of March 30, 2023, by the Italian Data Protection Authority (*Garante per la protezione dei dati personali*)**, which ordered a temporary limitation on data processing for national users against *OpenAI*, the US company behind well-known artificial intelligence software **ChatGPT**.

The Italian Garante identified two structural macro-violations of GDPR parameters:

- **Absence of Disclosure and Legal Basis:** ChatGPT failed to provide users with any clear disclosure regarding personal data collection. Furthermore, there was a structural **absence of any suitable legal basis** to justify the massive scraping and storage of personal information for the purpose of "training" the platform's underlying algorithms.
- **Lack of Age Verification Filters:** Despite the service being theoretically aimed at users over 13, the Authority noted a total absence of technical systems to verify a user's actual age, exposing minors to completely inappropriate software responses relative to their developmental stage and self-awareness.

This landmark intervention, which anticipated the strict criminal and administrative *compliance* requirements later introduced by the **European Artificial Intelligence Act (AI Act)**, opened a permanent debate on balancing algorithmic innovation with digital sovereignty and European citizens' core rights.

The centrality of protecting information assets within the Euro-unitarian space finds its ultimate fulfillment in civil liability paths for cyber-attack victims, extending data controllers' responsibility far beyond tangible financial loss alone.

**CASE STUDY**

**Court of Justice of the European Union, VB v. Natsionalna agentsia za prihodite, 2023**

With its judgment of December 14, 2023, in Case C-340/21, the Court of Justice of the European Union offered an important, innovative clarification regarding **recoverable non-material damage for GDPR violations** following a cyber-attack. The Luxembourg judges clarified that the **fear felt by a person** that their personal data, following a *data breach*, might be unlawfully used by third parties can, by itself, constitute a compensable non-material damage under **Art. 82 of the Regulation**.

It is therefore not necessary for the data subject to prove a concrete, already occurring abusive use of the data, or that the psychological injury has reached a statutory minimum threshold of severity. It is sufficient for the individual to prove they suffered a form of **distress, worry, or anxiety** linked to the actual risk that their personal data might be subject to misuse in the future. The Court specified that Art. 82(1) precludes a national practice that conditions compensation on a minimum gravity threshold of non-material damage, and that one cannot exclude from the very concept of non-material damage a situation where the data subject invokes the fear that their personal data will be subject to future misuse by third parties. This historic ruling raises the cyber-resilience standard for European businesses, forcing them to invest thoroughly in the security protocols mandated by the **NIS 2 Directive** to prevent class-action compensation claims by consumers.

## XIII. How Does the AI Act Regulate Defensive and Offensive Cybersecurity Technologies?

The evolution of **Artificial Intelligence (AI)** has had a disruptive impact on computer crime, introducing new attack methods that pose complex technical, criminological, and legal challenges. The contemporary cyber space of **2026** is configured as an asymmetric theater of conflict where AI is utilized both as an offensive weapon and a shield of predictive defense.

On the front of offensive threats, the use of **advanced generative AI systems** allows *cyber-criminals* to design and deploy **polymorphic and adaptive malware**. These malicious codes are capable of autonomously modifying their own strings and dynamically adapting to the operational environments into which they are inoculated, evading traditional detection mechanisms based on fixed digital signatures used by ordinary *antivirus* software. Added to this is the increasingly sophisticated use of social engineering (*social engineering*), enhanced by the automated, mass analysis of large amounts of personal and economic data from open sources (*OSINT*) or compromised databases (*data breach*). This allows eversive cells to create highly personalized fraudulent communications and *phishing* emails (*spear phishing*), increasing the effectiveness of the deception. Another particularly insidious expression of AI in the criminal context concerns the use of **deepfake** technology, which allows for the high-precision biometric simulation of real subjects' vocal, phonic, and visual appearances to carry out complex identity frauds and gain unauthorized access to protected systems.

Nevertheless, AI offers extremely powerful tools to reinforce cyber defenses, turning into a strategic ally for *cybersecurity*. Through the application of **predictive algorithms and Machine Learning models**, it is possible to analyze colossal volumes of network traffic in real time, quickly identifying anomalous behaviors or statistical deviations that indicate a cyber-attack is underway. This preventive detection capability allows for immediate mitigation action by CSIRTs, which is decisive in containing damage and isolating compromised servers before data encryption takes place. In the banking sector, the integration of AI into financial monitoring systems enables the identification of suspicious transactions and atypical account accesses, facilitating the adoption of **adaptive multi-factor authentication (MFA) measures**. Finally, AI proves indispensable in post-attack digital investigations (*incident response*), supporting forensic analysis, system log correlation, and the temporal reconstruction of intrusion dynamics.

In this technologically fluid context, the European Union's intervention through the adoption of **Regulation (EU) 2024/1689 (globally known as the AI Act)** holds a central dogmatic relevance, standing as the world's first comprehensive framework on artificial intelligence.

**REFERENCES**

**Regulation (EU) 1689, 2024, Recitals 4, 5, and 6**

The European legislator, in the introductory recitals of the AI Act, establishes the dual and anthropocentric philosophy of the rule:

**Systemic Benefits (Recital 4):** AI represents a fast-evolving family of technologies that brings a wide range of economic, environmental, and social benefits across the entire spectrum of industries and social activities. By improving forecasting, optimizing operations and resource allocation, and personalizing digital solutions, AI can provide key competitive advantages to companies and lead to beneficial social and environmental outcomes, such as in healthcare, infrastructure management, energy, transport, security, and justice.

- **Risks and Prejudices (Recital 5):** At the same time, depending on its specific application, utilization, and technological development, AI can generate risks and harm public interests and fundamental rights protected by Union law. Such harm can be both material and non-material, including physical, psychological, social, or economic injury.
- **The Anthropocentric Approach (Recital 6):** Given the significant impact AI can have on society and the need to build trust, it is essential that AI and its regulatory framework develop in accordance with Union values (Art. 2 TEU) and fundamental rights and freedoms (Art. 6 TEU, Charter). As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.

To translate these principles into binding legal obligations, the AI Act introduces a strict risk-based approach for classifying intelligent software. Systems intended to be used for the management and operation of **critical infrastructures** (such as water, gas, electricity, and transport networks), as well as those used by law enforcement for crime risk assessment or remote biometric identification, are strictly classified as **high-risk systems**. Such systems are subject to demanding technical and legal *compliance* obligations, including risk management systems, total training data traceability (*data governance*), technical robustness against external attacks (*cyber-resilience*), and mandatory **human oversight (*human-in-the-loop*)**.

The AI Act categorically prohibits AI systems presenting an unacceptable risk, such as subliminal behavioral manipulation practices or social scoring . This regulatory framework, coordinating in perfect tandem with the **NIS 2 Directive** and the **Cyber Solidarity Act**, responds to the need to ensure that European digital security is built on ethical, transparent, auditable, and legally sustainable foundations, guaranteeing that algorithmic innovation does not result in a violation of the rule of law.

**FOCUS**

**AI in Deepfakes and the Counterfeiting of Non-Cash Means of Payment**

The abuse of AI technologies and the creation of sophisticated audiovisual deepfakes constitute the operational arm for executing behaviors falling under other Eurocrimes under Art. 83 TFEU, with specific reference to the **Counterfeiting of non-cash means of payment** and **Organized crime**. In international financial fraud schemes, criminal syndicates use AI-assisted voice cloning (*voice cloning*) to simulate executives' directives over the phone (*CEO Fraud*), inducing accounting departments to transfer massive amounts of money to offshore bank accounts. The integration of intelligent monitoring systems mandated by the AI Act and banking supervision authorities (the European **AMLR** package) allows for the detection of atypical financial orders, blocking fraudulent transactions and severing the profit line of mafia organizations.

## XIV. How Can the Ambiguity of State-Sponsored Cyber-Attack Attribution Be Overcome?

The increasing integration of information technologies and offensive digital tools into national military strategies (a phenomenon known as ***cyberwarfare***) raises substantial legal and dogmatic issues regarding international responsibility for state-sponsored cyber operations. The primary challenge on a global scale relates to the **identification and accountability of the sovereign State** to which the hostile cyber act should be attributed, especially when it is programmatically executed to mask its origin. State-backed hacker groups and military agencies structurally exploit network anonymity, the use of non-state actors operating as intermediaries (*proxies*), or complex technological deception and obfuscation techniques, such as *proxy servers* and false flag operations (*false flag operations*).
In the absence of a specific and binding international treaty governing military operations in cyberspace, doctrine and practice refer to the **Draft Articles on Responsibility of States for Internationally Wrongful Acts** (UN International Law Commission, 2001).

**REFERENCES**

**International Law Commission, Draft Articles on State Responsibility, 2001, Art. 8**
The text establishes that the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting **on the instructions of, or under the direction or control** of that State in carrying out the eversive conduct.
However, the standard of technical and digital evidence required to legally prove such direct or stringent control (*effective control*) before international courts is extraordinarily complex to obtain. This fuels the so-called **attribution dilemma (*attribution dilemma*)**, hindering the activation of any legal response, retaliatory countermeasure, or official diplomatic sanction.

From the standpoint of public international law and the preservation of global peace, the qualification of a cyberattack clashes with the cornerstones of the UN Charter. **Art. 2, para. 4, of the United Nations Charter** expressly prohibits the threat or use of force in international relations between States. A cyberattack that causes structural damage equivalent to that resulting from a conventional kinetic military action–such as the coordinated collapse of vital civilian critical infrastructures (nuclear plants, power grids), direct civilian casualties, or the systemic paralysis of a country's telecommunications–falls within this notion of aggression, paving the way for the application of **Art. 51 of the same Charter**, which legitimizes the inherent right to **individual or collective self-defense** against an armed attack.

**FOCUS**

**The "Stuxnet" Malware Case, 2009**

The cyberattack known as **Stuxnet**, which occurred in 2009, is universally recognized by international law doctrine as the **first documented and tangible case of cyber warfare (*cyberwarfare*)**. The *malware*, the result of a joint intelligence operation likely attributed to the United States and Israel, had the geopolitical objective of **disrupting nuclear enrichment activities in Iran**, specifically targeting the Natanz military facility, home to the centrifuges for uranium enrichment. The attack stood out for its extremely high level of technical sophistication: inoculated via an infected USB flash drive to bypass networks isolated from the Internet (*air-gapped*), the virus altered the rotation speed of the centrifuges, causing their physical destruction, while displaying completely normal operating parameters on the technicians' monitors. Stuxnet thus succeeded in achieving a **concrete destructive effect on a military critical infrastructure**, without the deployment of conventional armed forces, missiles, or troops on the ground.

Beyond its direct effects on the Iranian facility, Stuxnet had a global impact, spreading uncontrollably and infecting industrial control systems (*SCADA*) in over one hundred countries. The event exposed the **systemic vulnerabilities of digitalized critical infrastructures**, revealing the absence, until then, of adequate protection and resilience mechanisms. The incident fueled the international debate on the necessity of legally regulating state conduct in cyberspace, especially when it is capable of producing effects comparable to a kinetic armed attack, configuring hypotheses of **unlawful use of force under Art. 2, para. 4, of the United Nations Charter**.

**FOCUS**

**Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013**

The ***Tallinn Manual*** **(drafted by a group of international experts under the mandate of the NATO Cooperative Cyber Defence Centre of Excellence)**, while not a binding legal treaty, constitutes the most authoritative interpretative framework for applying the international law of armed conflict to cyberspace. The Manual affirms the principle of **equivalence of effects**: a *cyber operation* constitutes an unlawful use of force under Art. 2(4) of the UN Charter if its physical effects and destructive consequences (injuries to persons or destruction of physical property, as historically demonstrated by *Stuxnet*) are analogous to those produced by traditional military operations or kinetic bombardments. This dogmatic equivalence, however, requires a rigorous case-by-case assessment, coordinating it with absolute respect for the principles of **proportionality, necessity, and distinction** between civilians and combatants should the attacked State decide to launch a retaliatory armed or digital response.

The legal uncertainty stemming from the lack of universally shared rules, combined with the technical difficulty of definitively identifying the digital perpetrator of an attack, makes it crucial to strengthen supranational mechanisms of transparency, adopt common standards for the **forensic preservation and cross-border sharing of digital evidence**, and draft an updated public international law framework capable of definitively closing the current regulatory gaps in cyberspace.

**FOCUS**

**The Tandem Between Cyberwarfare and Transnational Terrorism**

In today's geopolitical scenario, state-sponsored cyber warfare techniques regularly intertwine with the Eurocrime of **Transnational Terrorism** under Art. 83 of the TFEU. States acting as sponsors of global eversion (*State-sponsored terrorism*) provide military-grade spyware, cyber weapons, and attack instructions to terrorist cells or structured eversive groups. The latter execute cyberattacks against European Union institutions or financial systems, acting as a shield and allowing the mandating State to invoke **plausible deniability** to avoid retaliation under Art. 51 of the UN Charter. This demonstrates that countering state-sponsored *cybercrimes* requires immediate operational coordination between **Europol (EC3 Centre)**, defense intelligence agencies, and the **Cyber Solidarity.**

The legal flow of attribution and reaction in cyberwarfare takes place into 4 phases:

- **Phase 1 - The Cyber-Offensive Event:** Inoculation of a military-grade malware (e.g., the *Stuxnet* attack). Obfuscation of digital traces through *proxy* servers located in non-cooperative jurisdictions.
- **Phase 2 - Forensic and Technological Analysis:** Intervention of CSIRTs and military laboratories to isolate the source code and identify the digital footprint of the attack (*cyber-attribution*).
- **Phase 3 - Dogmatic Review (ILC Model / Tallinn Manual):** Verification of the command link under Art. 8 of the 2001 ILC Draft. Evaluation of the attack's impact: if analogous to a kinetic military aggression, it triggers a violation of Art. 2(4) of the UN Charter.
- **Phase 4 - Multilevel International Response:** Activation of diplomatic channels or, in cases of a systemic and lethal threat to the State's vital infrastructures, legitimization of a response in self-defense under Art. 51 of the UN Charter, backed by the **European Cyber Shield** of the Cyber Solidarity Act.

## XV. Key Findings

The scientific, historical, and regulatory analysis carried out within this paper leads to the outline of **six fundamental findings** that we must keep in mind for a complete understanding of the subject matter:

- **Cybercrime as a Complex and Evolving Phenomenon:** A cybercrime is configured when an active or passive digital conduct, carried out with awareness and **intent (*dolo*)**, damages or endangers legally protected assets, such as system integrity, data confidentiality, or economic property. The objectives pursued by transnational syndicates can be financial (e.g., *ransomware* ransoms), ideological (*hacktivism*), or personal (*revenge porn*), moving along a border between lawful and unlawful that is often blurred by the apparent neutrality of digital tools.
- **Global Regulatory Response and the Budapest Convention:** Historically, the lack of a unified definition and binding sanctions on an international scale favored the impunity of perpetrators, offering **"safe havens"** to cybercriminals due to the absence of the dual criminality principle, as highlighted by the *ILOVEYOU* virus of 2000. The **Budapest Convention (2001)** by the Council of Europe represented the first step toward a coordinated response and the typification of core offenses (*illegal access, data interference*), now enhanced by the adoption of the new **UN**

**Convention on Cybercrime of 2024**, aimed at guaranteeing universal accession and mandatory *capacity building* for developing nations.

- **Centrality of Domestic Italian Criminal and Procedural Protection:** The Italian legislator, from Law 547/1993 to Law 48/2008, transposed international standards by introducing specific offenses into the Criminal Code (Art. 615-*ter*, and Art. 640-*ter* c.c.). The jurisprudence of legitimacy (Supreme Court Judgment No. 40470/2018) extended penal protection by clarifying that the notion of a "computer system" is independent of a network connection, emphasizing the substantive functionality of the device. On a procedural level, **Art. 51, para. 3-*quinquies* of the Code of Criminal Procedure (c.c.p.)** centralizes investigative powers within District Prosecutor's Offices, ensuring high technical and digital-forensic specialization.
- **The Transition toward Cyber-Resilience and Mandatory Sharing:** European security policy supplements criminal enforcement with a structural pillar of technical prevention. The **Cybersecurity Act of 2019** granted a permanent mandate to **ENISA** and established the European certification framework for ICT products. This system is today completed by the **NIS 2 Directive (EU 2022/2555)**, which imposes strict risk management obligations along the *supply chain* and mandatory urgent notifications of significant incidents within 24 hours to secure the Union's economy and vital infrastructures against priority threats.
- **Essential Involvement of the Private Sector and Security Agencies:** Given the speed and transnational scale at which digital threats evolve, Europol and its specialized **EC3** center closely collaborate with private technology companies (*Big Tech* and *ISPs*). Through operational tools such as the strategic threat assessments of the **IOCTA** report and the operational arm of the **J-CAT** taskforce, the public-private partnership enables a two-way exchange of tactical *intelligence* and the execution of coordinated cross-border operations to dismantle malicious networks and clandestine servers.
- **Protection of Digital Rights, AI Act, and Cyberwarfare Frontiers (2026):** European cybersecurity is inextricably linked to the protection of the individual and fundamental rights. The **GDPR** guarantees concrete remedies (mandatory notifications of data breaches and the extension of compensation to **immaterial damage arising from the fear of future data abuse under CJEU Judgment C-340/21**), also acting as a shield against the commercial deployment of AI software (the Italian Privacy Guarantor's order against *OpenAI/ChatGPT* in 2023). With the entry into force of the **Cyber Solidarity Act in 2025**, the Union addresses priority threats through the *European Cyber Shield* and the transition toward post-quantum cryptography (PQC). Finally, in military contexts (*cyberwarfare*), the application of the 2001 ILC Draft Articles and the *Tallinn Manual* parameters becomes fundamental to resolve state attribution dilemmas highlighted by the *Stuxnet* case, defining the limits of the use of force and self-defense under Art. 51 of the UN Charter in cyberspace.

# Counterfeiting of Means of Payment

*by Francesco Foccillo*[*]

SUMMARY: I. What Is the Definition of Counterfeit Means of Payment? – II. Who Counterfeits Means of Payment? – III. How Is the Multilevel Harmonization Against Counterfeiting Articulated Under International Law? – IV. What Is the Role of INTERPOL in the Fight Against Counterfeit Currency? – V. How Does Europol Act Against the Counterfeiting of the Euro? – VI. How Is the Counterfeiting of Cash Means of Payment Regulated Under European Union Law? – VII. How Does European Regulation Govern the Counterfeiting of Non-Cash Means of Payment? – VIII. What Criminalization Obligations Are Imposed by Directive 2014/62/EU Regarding Currency Counterfeiting? – IX. Does The Graphic Design of Banknotes Affect the Fight Against Counterfeiting? – X. How Does the Italian Legal System Regulate the Counterfeiting of Means of Payment? – XI. How Can Technology and Artificial Intelligence Aid the Fight Against Counterfeiting? – XIII. How Is the Counterfeiting of Means of Payment Connected to Other Eurocrimes?

KEY FINDINGS: Evolution of the dogmatic notion; Dual track of euro-unitarian protection; Technological barriers and graphic safeguards; Hierarchical criminal structure and agency interoperability; Systemic interconnection and the cybercrime nexus.

## I. What Is the Definition of Counterfeit Means of Payment?

Given the absence of a unique definition of counterfeit means of payment in the Italian Criminal Code (which punishes such conduct through specific criminal provisions that will be discussed subsequently) and taking into account that this phenomenon presents uniform transnational traits, this paper refers to the definition used by the Australian legislator in the *Crimes (Currency) Act* of 1981, which remains in force as a comparative parameter.

**REFERENCES**

**Crimes (Currency) Act (Australia), 1981, Definitions Section**

The Australian legal system defines counterfeit money (using the term "money" in a broad sense to indicate means of payment) as: "any article, other than a genuine coin or paper money, that resembles, or is apparently intended to resemble or pass for, a genuine coin or paper money; or any article, although originally a genuine coin or paper money, that has been altered in a substantial way and such as to conceal, or be intended to conceal, the alteration itself".

[*] Ph. D. Student in Legal Sciences, Member of the Research Staff of the International & European Criminal Law Observatory (IECLO), University of Salerno, Italy

Starting from this dogmatic premise, we can define the **counterfeiting of means of payment** as the combination of all activities aimed at the **creation of false currency**. This definition is not exhausted in the mere material manufacture of the banknote or security, but encompasses the entire logistical chain and the **preparatory and functional phases**, such as the sourcing of special raw materials (e.g., watermarked paper, magnetic inks), the possession of the necessary technological tools, and the subsequent introduction and distribution of the counterfeit currency into economic channels.

**FOCUS**

**The Counterfeiting of Money as *Lesa Maestà***

The counterfeiting of money is a criminal phenomenon that arises concurrently with the introduction of the first mercantile means of payment. An emblematic historical case of anti-counterfeiting legislation is the ***Lex Cornelia de maiestate* of 81 B.C.**, enacted under Lucius Cornelius Sulla, which had among its primary objectives the limitation of the then rampant circulation of falsified silver coins (*nummi adulterini*), politically framing such conduct within the very grave **crime of *lesa maestà*** (literally **injured majesty**). This severe classification of falsification activity remained valid in legal dogmatics until the modern era, justified by the profound symbolic value of the imprint stamped on the metal: the coin, bearing the **"sign of the Prince"** and being a sovereign expression of the power of the State, rendered its alteration a direct attack on political authority and the stability of the sovereign. For example, *Section 1* of the *Counterfeiting Coin Act* of 1741, which remained in force in Great Britain from 1742 to 1832, included within the category of ***high treason*** the modification or fabrication *ex novo* of silver shillings or *sixpences* aimed at making them deceptively resemble the gold guinea, punishing offenders with the death penalty.

## II. Who Counterfeits Means of Payment?

In studying multilevel enforcement strategies against counterfeiting, it is essential to accurately identify the subjects and groups operating in this sector, analyzing their structural differences in *modus operandi* and underlying economic-political motivations. We must remember that the phenomenology of counterfeiters is articulated into **three distinct macro-categories**:

1. **Independent Counterfeiters:** These are individuals or small isolated groups not affiliated with large organized crime cartels. Their activity is today heavily conditioned and limited by the **increasingly innovative technological and biological security features** introduced by central banks (e.g., holograms, polymers). However, these subjects attempt to evolve in step with advancements in commercial high-resolution laser printing technologies, accessible even to counterfeiters with low financial resources. The conducts of these groups, if structured, are punishable in Italy under **Art. 416 of the Criminal Code (conspiracy/criminal association)**. Independent counterfeiters usually generate a limited negative impact on the market, characterized by a quantitatively low production and a predominantly **local or regional** distribution and dealing network.
2. **Structured Criminal Organizations:** This category includes large cartels and mafia-type associations (including terrorist organizations) that utilize advanced industrial printing techniques, such as **lithographic or intaglio printing**, sometimes accessing professional machinery through the infiltration or complicity of legitimate printing companies unaware of the actual illicit use. These

organizations counterfeit means of payment primarily as an asymmetric tool to **self-finance other illicit activities** with high logistical costs (e.g., drug trafficking or weapon purchasing), as historically demonstrated by Colombian cartels and Middle Eastern eversive cells.

3. **State or Para-State Actors:** This third category consists of sovereign States or para-state organizations that print counterfeit foreign currency as a true **tool of political-economic sabotage** against their geopolitical enemies (for instance, to induce artificial monetary inflation, destroy market confidence, or destabilize the purchasing power of the target currency) or as a means of covert international financing to bypass sanctions regimes. Disposing of unlimited financial and technological resources, these actors are capable of producing counterfeits of the **highest forensic quality**, sometimes entirely indistinguishable from the originals except through in-depth spectrographic laboratory analyses.

**FOCUS**

**The Phenomenon of North Korean "Superdollars"**

An outstanding example of international practice and global financial intelligence relations is the famous case of the so-called **"Superdollars"**. In 1996, the *New York Times* published a detailed article denouncing that the Democratic People's Republic of Korea had produced, in the preceding decades, $100 banknotes of exceptionally high quality, injecting them into the global circuit through its consular and diplomatic missions. These counterfeits were made using highly sophisticated technologies–including the use of paper composed of 75% cotton and 25% linen, magnetic inks, and intaglio printing–rendering them virtually indistinguishable from originals and surpassing ultraviolet tests and bank counting machinery of the era. It is estimated that this activity, officially denied by Pyongyang, generated hundreds of millions of dollars to fund the regime's activities, bypass international sanctions, and sustain military programs. Although the Federal Reserve radically redesigned the $100 bill in 2013 to counter this phenomenon, suspicions regarding a resumption of production re-emerged between **2024 and 2026**.

The structure of criminal organizations dedicated to large-scale counterfeiting is complex and articulated into a **pyramidal and compartmentalized hierarchy** to reduce the risk of infiltration by judicial police organs:

- **The Printers (*Producers*):** They constitute the technical apex; they are responsible for the physical production of the currency through clandestine industrial laboratories. They sell the banknotes wholesale at approximately **20-25% of the face value**.
- **The Distributors (*Wholesalers*):** They manage the macro-regional flows of counterfeit currency, purchasing batches from the printers and organizing the storage and transborder transfer.
- **The Retailers (*Passers*):** Affiliates of the organization who physically inject and launder the banknotes into the consumer market through front commercial activities or currency dealing squares.
- **The Mules (*Couriers*):** Subjects tasked with the **physical cross-border transport** of the counterfeit currency, splitting loads to overcome customs checks at the borders of the Union. The final price for the end user or buyer can reach **65-75% of the face value**.

## III. How Is the Multilevel Harmonization Against Counterfeiting Articulated Under International Law?

Data showing the intrinsically transnational nature of counterfeiting means of payment–a phenomenon that knows no geographical borders or temporal barriers–rendered an articulated regulatory activity at a global level necessary. The first universal regulatory pillar dates back to 1929 when, under the aegis and auspices of the League of Nations, the International Convention for the Suppression of Counterfeiting Currency was drafted, known in the Italian legal system as the **International Convention for the Fight against the Falsification of Currencies** (signed in Geneva on April 20, 1929).

The Convention, which entered into force on February 22, 1931, and was ratified by Italy through Law no. 2283 of November 23, 1935 (in force since December 27, 1935), defines in Art. 2 "currency" as: "both paper money, including banknotes, and metallic money, which are legal tender by virtue of a law". This definition, although innovative and a milestone for the time in introducing a common legal lexicon among signatory States, reflected the economic and commercial reality of the era. We must remember that the first mass-consumption credit card would only be devised in 1949, rendering the 1929 Convention temporally distant and structurally devoid of references to modern electronic or digital payment systems.

The treaty stems from the firm conviction of States that currency counterfeiting constituted a true *crimen iuris gentium* and that purely national enforcement actions were completely insufficient, if not technically impossible, creating dangerous zones of impunibility for counterfeiters. This treaty instrument remains, even today, the primary international point of reference and the historical source of cooperation in this field. The need for multilateral coordination is dictated by the sophisticated operational strategies of cartels, such as the international trafficking of counterfeit currency and the production of banknotes outside the sovereign jurisdictions that issue them. Consistent flows of counterfeit US dollars have been historically located and monitored in Colombia, Peru, Israel, the geopolitical area of the Caucasus, and West Africa.

Recently, in **2024 and 2025**, international cooperation has further evolved through the **strengthening of the operational protocols of INTERPOL and Europol**, aimed at countering not only traditional physical cash, but also the counterfeiting of non-cash payment instruments, such as cloned credit cards, electronic wallets (*e-wallets*), and non-monetary digital transactions, in line with new European directives on *cybersecurity*.

**REFERENCES**

**International Convention for the Suppression of Counterfeiting Currency, 1929, Art. 3**

"The following should be punishable as ordinary crimes: 1. Any fraudulent making or altering of currency, whatever means are employed; 2. The fraudulent uttering of counterfeit currency; 3. The introduction into the country, the receiving or obtaining of counterfeit currency, knowing it to be counterfeit, with a view to its uttering; 4. Attempts to commit, and any intentional participation in, these offenses; 5. The fraudulent making, receiving or obtaining of instruments or other articles peculiarly adapted by their nature for the counterfeiting or altering of currency."

In more recent times, within the UNTOC (Palermo, 2000), the counterfeiting of means of payment is not explicitly cited. On the contrary, in the legal system of the European Union, it is expressly provided for by Art. 83, Para. 1, TFEU, which lists the so-called

Eurocrimes. These are defined as "areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offenses or from a special need to combat them on a common basis".
In addition to the counterfeiting of means of payment, the list includes: "terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, computer crime, and organized crime". For such crimes, the European Parliament and the Council may establish, by means of directives, minimum rules concerning the definition of criminal offenses and sanctions.
On the front of technological development in anti-counterfeiting, the **Central Bank Counterfeit Deterrence Group (CBCDG)**, established on May 10, 2000, brings together the governors of 35 central banks (including the European Central Bank) with the objective of examining the threats posed by new digital technologies. The work of the CBCDG led, in 2004, to the birth of the **Counterfeit Deterrence System (CDS)**: a set of technologies designed to prevent image processing software and personal computing tools from capturing and reproducing images of protected banknotes.

**CASE STUDY**

**Supreme Court of the Philippines, Judgment No. 261670, 2023**
A confirmation of the current application of the principles enshrined in Art. 3 of the International Convention for the Suppression of Counterfeiting Currency (which mandates the punishability of possession and uttering of false currency) is traceable in the case ***Gacasan v. People***. In this setting, the Supreme Court of the Philippines confirmed the prison sentence for Allan Gacasan, found in possession of 100 counterfeit 1,000-Peso banknotes and 25 counterfeit 500-Peso banknotes. The defendant had accepted a purchase offer made by a law enforcement officer engaged in an undercover operation (*buy-bust operation*). The judgment reiterates that the mere possession of false currency with the intent to utter it constitutes a serious crime, in line with international anti-counterfeiting standards established by the 1929 Convention.

## IV. What Is the Role of INTERPOL in the Fight Against Counterfeit Currency?

The **International Criminal Police Organization (INTERPOL)** is an intergovernmental entity dedicated to strategic cooperation between the police forces of its Member States and the operational countering of transnational crime. Nearly all countries in the world belong to it (among UN members, only North Korea and the Federated States of Micronesia have not yet joined), facilitating the real-time sharing of data and criminal intelligence information essential for collective security.
In the area of counterfeiting means of payment, INTERPOL's activities focus mainly on three operational guidelines that the must be remembered: **technical and forensic support**, **specialized training** for territorial law enforcement, and the **coordination of joint international operations** aimed at dismantling clandestine printing facilities and seizing false currency before its injection into the market.
In addition to these field services, INTERPOL makes several informational resources available online:

- ***Counterfeit alerts*:** Information and forensic analysis on new types of counterfeit banknotes identified on the global market (excluding the euro and US dollars, which are managed by specific channels and dedicated agencies).

- **Annual statistics and reports:** Analytical data regarding the total quantities and types of counterfeit banknotes discovered and seized by Member States.
- ***Early warning messages*:** Urgent notices regarding euro counterfeiting, published and distributed in close cooperation with **Europol** and the **European Central Bank (ECB)**.
- ***Document-checker banknotes*:** A centralized online database containing **4,800 types of banknotes** and over **70,000 high-resolution images** to support the visual and instrumental checks of border agents.

Advanced technical analyses are carried out at the *Counterfeit Currency and Security Documents laboratory*. This facility is responsible for analyzing, cataloging, and archiving both newly issued legal banknotes (to study their security features) and counterfeit ones seized across different continents, producing technical reports in forensic chemistry. These activities reflect INTERPOL's strategic vision, which in its annual report has placed the fight against counterfeiting among the **priority objectives** to weaken the financial capabilities of mafia organizations.

Within the framework of advanced prevention, an initiative of international importance is **Project S-Print**, aimed at monitoring the commercial supply chain of industrial materials and sensitive equipment (e.g., intaglio presses, magnetic inks, watermarked paper). The objective is to support legitimate supply companies that, while acting in good faith, might sell industrial machinery to buyers operating under false pretenses or through front companies to evade the controls of law enforcement.

**FOCUS**

**The Guidelines of Project S-Print**

Through the *Project S-Print Best Practices*, INTERPOL provides a set of **operational recommendations and conduct standards** to actors in the chemical-typographic production chain to prevent machinery, special inks, or paper substrates from being exploited by forgery cartels. These guidelines are articulated into five due diligence duties:

**1. Maintain complete records:** Keep detailed accounting and technical documentation of all transactions and machinery specifications sold.

**2. Customer profiling (*Know Your Customer*):** Verify the true identity of each new buyer, cross-checking the information provided with independent, objective sources and commercial registries.

**3. Commercial precautionary principle:** Refrain from supplying materials or technologies in case of minimal doubts regarding the legitimacy of the customer or the proposed real destination of use for the instrumentation.

**4. Direct cooperation with authorities:** Promptly report to police forces and INTERPOL contact points any anomalous order or suspicious commercial contact.

**5. Secure disposal of materials:** Provide for the traceable destruction or responsible disposal of obsolete equipment, printing plates, or waste materials, to prevent their illicit recovery and reuse by criminal organizations.

In conclusion, the **forensic and digital resources of INTERPOL** are:

- **Counterfeit Currency Laboratory:** Hub for chemical and forensic analysis on falsified inks, paper, and holograms.
- **Document-Checker Database:** Centralized digital archive for customs support with 4,800 types of banknotes and 70,000 comparative images.
- **Early Warning Messages (ECB-Europol):** Rapid alert system for intercepting massive flows of false euros within the common space.

- **Project S-Print Network:** Multilevel preventive system for monitoring the supply chain and technological precursors of printing.

## V. How Does Europol Act Against the Counterfeiting of the Euro?

The action of the **European Union Agency for Law Enforcement Cooperation (Europol)** is closely interconnected with that of INTERPOL. This operational coordination is enshrined in the ***Joint Initiative*** **between the Secretary General of INTERPOL and the Director of Europol** on the fight against currency counterfeiting, with specific reference to the euro, signed on November 5, 2001, just before the physical entry into circulation of the single currency. The *Joint Initiative* stems from the broader Cooperation Agreement between the two agencies and arises from the need to deepen investigative synergy in the specific sector of false currency. The document is articulated in four fundamental articles regulating the direct exchange of information (Art. 2), requests for technical assistance (Art. 3), and operational coordination on the field (Art. 4).

In 2005, **Council Decision 2005/511/JHA** took a decisive step by officially designating Europol as the "**central office for the fight against the counterfeiting of the euro**", within the meaning of the 1929 Geneva Convention. This fundamental act confers upon the agency the task of centralizing investigations, analyzing strategic intelligence information, and facilitating judicial and police cooperation between the security forces of Member States.

In the conclusions of the Council of the EU defining the priorities of the Union against organized crime, the fight against criminal organizations involved in the production and distribution (both physical and online) of counterfeit money was confirmed as a priority objective of the permanent **EMPACT (European Multidisciplinary Platform Against Criminal Threats)** program. EMPACT represents the platform for multidisciplinary cooperation led by Member States and supported by EU institutions and agencies, including Europol itself, to dismantle the chains of command of transnational forgery associations.

**FOCUS**

**Two Counterfeiting Operations by Europol**

The effectiveness of the EMPACT operational model in targeting not only physical typographic production but also the new digital distribution channels used by organized crime is demonstrated empirically by two major recent investigations:

**1. Dismantling of the Naples printing facility (August 14, 2024):** Facilitated by the exchange of information and coordinated by Europol, the French *Police Nationale* and the Carabinieri Corps in Italy dismantled a sophisticated clandestine printing facility in Naples. The operation led to the seizure of high-quality counterfeit banknotes with a face value of approximately **3 million euros**. The laboratory, hidden behind a mobile wall electronically operated in a private garage, was equipped with 31 digital printing machines and large quantities of raw materials. It is believed that the arrested forger was responsible for the production of **over 27% of all false banknotes** of 20, 50, and 100 euros removed from circulation in the entire eurozone during 2023.

**2. Cross-Border Operation (April 7, 2025):** Europol supported a cross-border operation led by the Italian Carabinieri with the support of the authorities of Austria, Belgium, France, Germany, and Spain. The investigation led to the arrest of three Italian suspects and the dismantling of a laboratory in southern Italy that distributed false currency throughout the eurozone via **online messaging platforms and encrypted applications**, accepting anonymous payments in **cryptocurrency**. During the intervention, 600 banknotes were seized for a total value of approximately 50,000 euros, alongside the dismantling of an illegal mint dedicated to coining 2-euro coins located in northern Italy.

## VI. How Is the Counterfeiting of Cash Means of Payment Regulated Under European Union Law?

The legislative activities of the European Union in the area of falsification underwent a substantial development with the introduction of the euro, the single currency that required common and homogeneous efforts to guarantee its effective protection. In Union law, the cornerstone regulation governing the fight against cash counterfeiting is **Council Regulation (EC) No 1338/2001** of June 28, 2001.

This regulation defines the measures necessary for the protection of the euro against counterfeiting and aims, as stated in Art. 1, Para. 1, to establish certain measures necessary for the circulation of euro banknotes and coins under conditions that guarantee their protection against counterfeiting activities. Art. 2 of the same regulation provides the technical definitions of "counterfeit banknotes and coins," distinguishing them from authentic ones based on their fraudulent manufacture or alteration. The regulatory framework was subsequently integrated by **Directive 2014/62/EU**, which harmonized minimum criminal penalties and introduced more incisive investigative tools across all Member States.

The new EU regulatory package against money laundering (**AMLR - Anti-Money Laundering Regulation**) has further strengthened the protection of cash, integrating the reporting mechanisms for suspicious banknotes provided for by Regulation 1338/2001 with the controls of banking supervisory authorities to limit the use of counterfeit currency in healthy legal commercial channels, initiating the integration of security standards for the future coexistence between physical cash and the **digital euro**.

**REFERENCES**

**Regulation (EC) 1338, 2001, Art. 1 para. 2**
The cited Regulation (EC) No 1338/2001 defines "counterfeiting" by covering both the fraudulent manufacture or alteration of banknotes and coins, and their uttering, importation, transport, and possession. The definition also extends to the possession of materials, computer programs, or tools suitable for the production or alteration of euro banknotes and coins or their protection features, regardless of the means utilized.

The regulatory extension to non-Euro States and AMLR integration has been organised in the following way:

- **Council Regulation (EC) No 1339/2001:** Extends the application of Articles 1 to 11 of Regulation (EC) No 1338/2001 (as amended by Regulation no. 44/2009) to all EU Member States that have not adopted the euro as their single currency, ensuring a uniform level of protection across the entire community territory and preventing legislative blind spots.
- **AMLR Package Alignment (2024-2026):** Integrates the technical reporting of suspect banknotes with the mandatory due diligence controls of commercial banks and financial entities in all Member States, including non-euro area countries, connecting cash anti-counterfeiting tracking with Central Bank supervisory systems.

## VII. How Does European Regulation Govern the Counterfeiting of Non-Cash Means of Payment?

European regulation for combating the counterfeiting of non-cash means of payment originates with Framework Decision 2001/413/JHA. However, due to accelerated technological evolution and the need to include new phenomena of cybercrime such as computer fraud and financial credential theft, this act was replaced by **Directive (EU) 2019/713**. The latter, pursuant to Art. 1, establishes **minimum rules concerning the definition of criminal offenses and sanctions** in the area of fraud and counterfeiting of non-cash means of payment, facilitating prevention and support for victims of digital fraud within the common space.
**Legislative Decree no. 184 of November 8, 2021,** constitutes the fundamental act transposing the Directive into the Italian legal system. Art. 1, letter a) of the cited decree defines a "**non-cash payment instrument**" as a non-cash protected device, object or record, material or immaterial, or a combination thereof, which enables the holder to transfer money or monetary value, including through digital means of exchange. This comprehensive definition includes not only physical cards, but also virtual currencies and digital assets.
Under the internal sanctioning profile, Legislative Decree 184/2021 profoundly innovated **Art. 493-*ter* of the Criminal Code**, which punishes the **unlawful use and falsification of credit cards, payment cards, or any other similar instrument**. The rule provides for imprisonment from one to five years and a fine from 310 to 1,550 euros for anyone who, in order to gain a profit, makes unlawful use of such instruments without being the holder. In the two-year period **2024-2025**, the application of this discipline was further strengthened at the European level to counter the phenomenon of large-scale *phishing* and *carding*. Furthermore, with the advancement of projects on the **digital euro** underway

between **2025 and 2026**, the regulatory framework is evolving to guarantee that new electronic payment instruments enjoy the same criminal and technological protection currently reserved for physical transactions and traditional cards.

**CASE STUDY**

**Court of Cassation, Fifth Penal Section, Judgment No. 34768, 2022**

The Court of Cassation clarified that Art. 493-*ter* c.c. finds application also in the event that a subject unlawfully uses a credit card received legitimately from the holder for a specific purpose, but employs it to carry out further and unauthorized operations (such as cash withdrawals for their own benefit). According to the judges of legitimacy, such conduct does not integrate the crime of embezzlement (Art. 646 c.c.), since the agent never acquires the legal "possession" of the card, but rather a mere precarious detention, strictly limited in time and in the purposes delegated by the holder. Therefore, the use of the device outside the limits of the mandate configures the crime of unlawful use of payment instruments, punished more severely precisely to safeguard the security of financial circuits and public trust.

**Council Regulation (EC) No 974/98**, on the introduction of the euro, parallelly addresses cash protection in Art. 12, establishing that participating Member States must ensure adequate sanctions against the alteration and falsification of banknotes and coins. Subsequently, on May 29, 2000, the European Union defined specific minimum rules through **Framework Decision 2000/383/JHA**, adopted in consistency with the aims today expressed by Art. 83 TFEU. This act emphasized the urgency of protecting the euro with effective criminal law measures even before its actual entry into circulation (which occurred on January 1, 2002) to defend the credibility of the new currency and avoid serious economic repercussions.

**REFERENCES**

**Framework Decision 383/JHA, 2000, Art. 3**

"Each Member State shall take the necessary measures to ensure that the following conducts are punishable offenses: a) any fraudulent making or altering of currency, whatever means are employed; b) the fraudulent uttering of counterfeit currency; c) the importation, exportation, transport, receiving, or obtaining of counterfeit currency with a view to its uttering; d) the fraudulent making, receiving, obtaining, or possession of instruments, objects, or computer programs peculiarly adapted by their nature for the counterfeiting or altering of currency, or of holograms and protective elements. Each Member State shall also ensure that participation, instigation, and attempts are passable by sanctions."

The protection of the euro from counterfeiting was further deepened in 2001 with **Council Decision 2001/887/JHA**. Given the need to integrate and strengthen the protection system, Art. 2 requires Member States to provide for the necessary expert analyses of suspect currency through a **National Analysis Centre (NAC)** for banknotes and a **Coin National Analysis Centre (CNAC)** for metallic currency, with the obligation to communicate the results of such assessments to Europol (Art. 3).
In the field of technical analysis of metallic coins, **Decision 2003/861/EC** provided for the establishment of the **European Technical and Scientific Centre (ETSC)**, whose activities were extended to non-euro area States by Decision 2003/862/EC. The ETSC was formally established by Commission Decision of October 29, 2004, with the objective of coordinating the technical actions necessary to protect euro coins against falsification. In 2014, European regulation became even more stringent: **Directive 2014/62/EU** established minimum rules concerning the definition of criminal offenses

and sanctions in the area of counterfeiting of the euro and other currencies, updating the list of offenses originally drafted in Framework Decision 2000/383/JHA, introducing more effective investigative tools, and harmonizing the statutory levels of penalties across the Union.

In conclusion, the institutional framework of EU expert analyses and enforcement is made up of:

- **Directive (EU) 2019/713:** Introduces minimum rules and legally defines non-cash payment instruments, covering also digital assets (transposed in Italy by Legislative Decree 184/2021).
- **National Analysis Centres (NAC & CNAC):** State bodies appointed for urgent technical expertise on suspect banknotes and coins, with an obligation to report to Europol under Decision 2001/887/JHA.
- **European Technical and Scientific Centre (ETSC):** Established in 2004 to coordinate at a central level the analytical response and protection against the counterfeiting of metallic euro coins.
- **Directive 2014/62/EU:** Updates the catalog of Eurocrimes linked to false cash currency, raising the minimum statutory sanctions to hinder penal *forum shopping*.

## VIII. What Criminalization Obligations Are Imposed by Directive 2014/62/EU Regarding Currency Counterfeiting?

The framework of Euro-unitarian sources safeguarding cash consolidated through **Directive 2014/62/EU**, which established minimum rules concerning the definition of criminal offenses and sanctions in the area of counterfeiting of the euro and other currencies, replacing and tightening the old framework of Framework Decision 2000/383/JHA. This source of European law imposes mandatory criminalization obligations to strike not only at production, but at the entire logistical and technological chain of false currency.

**REFERENCES**

**Directive (EU) 62, 2014, Art. 3**

"1. Member States shall take the necessary measures to ensure that the following conduct constitutes a criminal offense, when committed intentionally: a) any fraudulent making or altering of currency, whatever means are employed; b) the fraudulent uttering of counterfeit currency; c) the importation, exportation, transport, receiving or obtaining of counterfeit currency with a view to its uttering; d) the fraudulent making, receiving, obtaining or possession of: i) instruments, articles, computer programs and data, and any other means peculiarly adapted by their nature for the counterfeiting or altering of currency; or ii) security features, such as holograms, watermarks or other components of currency that serve to protect against counterfeiting. 2. Member States shall take the necessary measures to ensure that the conduct referred to in paragraph 1, points (a), (b) and (c), is punishable also in respect of banknotes or coins manufactured by using legal facilities or materials in violation of the rights or the conditions under which competent authorities may issue currency. 3. Member States shall take the necessary measures to ensure that the conduct referred to in paragraphs 1 and 2 is punishable also in respect of banknotes and coins which are not yet issued but are designated for circulation as legal tender."

The **European Central Bank (ECB)**, in its capacity as the issuing institution, has focused its regulatory efforts on the protection of the euro since 1998. These initiatives found a first foundation in Art. 4 of ECB Recommendation BCE/1998/7 of July 7, 1998. The document suggested a revision of enforcement policies in order to harmonize criminal law, enhance institutional and judicial cooperation, draft new conventions, and analyze the impact of new technological means available for counterfeiting.
In the same year, the ECB established the **Counterfeit Analysis Centre (CAC)**, the nerve center for the technical analysis of false banknotes. In addition to direct monitoring, the ECB offers strategic support to the private sector: companies producing control devices can test their machinery using a representative selection of seized counterfeit banknotes. Subsequently, the ECB publishes the list of instruments that have passed the tests, with the dual objective of guiding buyers toward reliable devices and stimulating manufacturers to develop increasingly sophisticated technologies. In the period **2024-2026**, this technical surveillance role became even more central in view of the project for the digital euro, requiring the ECB to integrate the protection of physical cash with new security standards for electronic transactions.

## IX. Does The Graphic Design of Banknotes Affect the Fight Against Counterfeiting?

Yes, design represents a fundamental technical security asset, not merely an aesthetic one, aimed at inhibiting counterfeiting through complex features and innovative materials. The actions of the ECB are not limited to institutional recommendations or the activities of the Counterfeit Analysis Centre; to these is added the initiative most visible to citizens: the design and restyling of banknotes.
Each year, the ECB publishes a report on counterfeit euro banknotes withdrawn from circulation. The report for 2024 indicates a ratio of **18 counterfeits for every million authentic banknotes**. Although this figure is slightly higher than in the preceding four-year period, it remains significantly lower than pre-Covid levels (23 per million in 2019) and far from the negative record of 64 per million registered in 2009. The ECB defines this share as "very small", confirming the effectiveness of current security measures.

## X. How Does the Italian Legal System Regulate the Counterfeiting of Means of Payment?

The counterfeiting of means of payment is not configured by the Italian legal system as a single omnibus criminal offense; the legislator explicitly distinguishes the counterfeiting of traditional cash (banknotes and coins) from that of instruments of payment other than cash (already analyzed under the regulatory scope of Directive 2019/713 and Legislative Decree 184/2021).
The counterfeiting of "national or foreign coins and banknotes, having legal tender in the State or abroad" and their fraudulent alteration are punished by **Art. 453 of the Italian Criminal Code** with imprisonment from three to twelve years and a fine from 516 to 3,098 euros. This statutory provision relates specifically to cash physical currency.

**REFERENCES**

**Italian Criminal Code, Art. 453**
"Whoever counterfeits or alters national or foreign banknotes or coins having legal tender, or introduces them into the territory of the State, or holds them with the intent to put them into circulation, shall be punished with imprisonment from three to twelve years and a fine from 516 to 3,098 euros."

## XI. How Can Technology and Artificial Intelligence Aid the Fight Against Counterfeiting?

Given the persistent and highly sophisticated circulation of fake currency, it is essential to understand how to detect counterfeit banknotes and coins, both as an advanced enforcement measure and for individual self-protection. Knowing how to recognize authentic money is also crucial on a strictly legal level: **Art. 457 of the Italian Criminal Code** punishes anyone who spends or puts into circulation counterfeit coins or banknotes received in good faith, providing for a penalty of imprisonment up to six months or a fine up to 1,032 euros.
To support citizens and retailers, the European Central Bank (ECB) provides an interactive section dedicated to security features. The primary "analog" barrier remains the **"feel, look, tilt"** method:

- **Feel:** Verifying the unique crisp texture of the paper made of pure cotton fibers and the raised intaglio printing on the edges.
- **Look:** Examining the watermark and the vertical security thread by holding the banknote against the light.
- **Tilt:** Observing the color-shifting effects of the emerald number and the appearance of Europa's portrait in the holographic window when tilting the bill.

However, for a deeper forensic analysis, technology enters the field. The most widespread physical and chemical detection tools include ***fake note detectors*** (fixed professional scanners verifying ultraviolet, magnetic, and metallic properties of banknotes) and ***counterfeit detector pens*** (iodine-based markers that react to the starches of common wood-based paper, turning dark, while remaining completely clear on authentic cotton-fiber banknotes, though proving ineffective for polymer plastic currencies like Australian bills).
The true technological revolution in the **2024-2026** period is represented by the integration of **Artificial Intelligence** and *Machine Learning*. Recent scientific studies have demonstrated that AI can make currency validation faster, more accurate, and globally accessible. In particular, systems based on **Convolutional Neural Networks (CNN)**, specialized in image recognition, have shown accuracy rates exceeding 82% even on limited datasets, with exponential growth potential as data volume increases.

**FOCUS**

**Future Developments and Banknote Verification via Smartphones**

A fundamental milestone in the use of AI for detecting counterfeit currency was achieved in **2025** by a research team at *Amity University*. The team developed a mobile application capable of verifying the authenticity of banknotes in real time **using nothing more than a standard smartphone camera**. This system bypasses the structural limits of traditional methods: unlike *Fake Note Detectors* (which are non-portable and expensive) and *Counterfeit Detector Pens* (which are inaccurate and unusable on polymers), the app guarantees immediate results and high scientific reliability. The native integration of an **automated voice assistant** transforms this technology into a powerful tool for social inclusion, allowing visually impaired or blind users to verify the authenticity of money in total autonomy. According to the developers, the system achieved a **95% accuracy rate** on a dataset of ten thousand images. This innovation paves the way for the capillary distribution of preventive anti-counterfeiting tools directly into the hands of citizens, transforming a common mobile device into a technological safeguard protecting public trust.

In conclusion, there are three levels of currency verification:

- **Level 1 - Sensory Verification (ECB Method):** Immediate check based on the three tactile and visual actions of "feel, look, tilt" accessible to every citizen.
- **Level 2 - Chemical/Physical Verification (Pens and Scanners):** Iodine reaction on wood starches and fixed ultraviolet/magnetic scanners for retail businesses and banks.
- **Level 3 - Digital/Cybernetic Verification (CNN Neural Networks):** Visual analysis via machine learning algorithms and mobile applications (Amity University 2025 Model) featuring inclusive voice guides and 95% accuracy.

## XII. How Is the Counterfeiting of Means of Payment Connected to Other Eurocrimes?

The counterfeiting of means of payment is not an isolated criminal phenomenon, but is deeply interconnected with other **Eurocrimes under Art. 83, Para. 1 of the TFEU**, serving primarily as an economic engine and a subsidiary logistical tool for funding and sustaining further large-scale illicit activities, such as drug trafficking, trafficking in human beings, and arms smuggling.

We must keep in mind the **four core areas of transnational criminal intersection**:

- **Terrorism and Narco-terrorism:** Terrorist organizations utilize currency counterfeiting both as a primary channel for logistical self-financing and as an asymmetric weapon of geopolitical destabilization. The massive injection of counterfeit currency into a targeted State's economy is programmatically aimed at generating artificial inflation, devaluing the legal tender, and undermining public trust in financial institutions.
- **Money Laundering:** From an economic criminal law standpoint, the **Financial Action Task Force (FATF/GAFI)**, in its Recommendation 3, classifies currency and means of payment counterfeiting as a **predicate offense** for money laundering. The financial proceeds generated from the wholesale distribution of fake currency constitute illicit capital that mafia consorteries must "clean" through legitimate commercial circuits to reinvest them in the legal economy.
- **Computer Crime (*Cybercrime*):** The technological evolution of digital payments has partially shifted the criminal axis from traditional print-shop falsification

toward sophisticated cyber-frauds, such as *skimming* (tampering with and cloning ATM and POS devices) and cross-border fraud on *e-commerce* platforms. An emerging phenomenon of high social alarm monitored by security agencies is ***crypto-counterfeiting***: by exploiting structural vulnerabilities and bugs in *blockchain* protocols, cyber-criminals succeed in generating duplicated tokens or executing fraudulent *double-spending* operations. Although the **MiCA (Markets in Crypto-Assets) Regulation 2023/1114** comprehensively disciplines crypto-asset markets, the **2024–2026** period has highlighted the urgent geopolitical need to integrate this framework with specific criminal enforcement measures against digital counterfeiting, given the structural absence of a central banking governance in the virtual currency sector.

- **Transnational Organized Crime:** Large criminal syndicates (such as the specialized counterfeit districts or Eastern European networks) manage the international trafficking of fake banknotes using the same logistical channels as legitimate cash and narcotics, relying heavily on physical *cash couriers*. The final insertion and "washing" of the currency into the retail market typically occur through cash-intensive businesses (restaurants, arcades, laundromats, retail chains), which inherently facilitate the mixing and confusion of legitimate and illicit capital.

## XIII. Key Findings

- **Evolution of the Dogmatic Notion:** The counterfeiting of means of payment has undergone a profound historical transition. Codefied since Roman times (*Lex Cornelia de maiestate*) and early modern English law (*Counterfeiting Coin Act* of 1741) as a severe crime of high treason due to the direct attack on the sovereign's effigy, it is today established as a **Eurocrime under Art. 83, Para. 1 of the TFEU**, protecting market stability, public trust, and the integrity of European financial circuits.
- **Dual Track of Euro-unitarian Protection:** The European Union protects payment instruments through a double regulatory architecture: physical cash (euro) is safeguarded by **Regulation (EC) No. 1338/2001** and the minimum rules of **Directive 2014/62/EU**; conversely, non-cash instruments (credit cards, electronic wallets, and digital assets) are covered by **Directive (EU) 2019/713**, transposed internally by Legislative Decree 184/2021, which significantly hardened **Art. 493-*ter* of the Italian Criminal Code**.
- **Technological Barriers and Graphic Safeguards:** The graphic and material design of banknotes serves as an advanced security presidium. The European Central Bank (ECB) integrates periodic iconographic restyling (such as the third series of Euro banknotes announced on January 31, 2025) with automated technical blocks managed by the CBCDG group, notably the **EURion constellation** pattern which, in synergy with the *Counterfeit Deterrence System* (CDS), technologically inhibits commercial software and hardware from scanning or printing currency images.
- **Hierarchical Criminal Structure and Agency Interoperability:** Large-scale currency falsification is run by structured, compartmentalized syndicates of producers, wholesalers, retailers, and couriers, with profit margins expanding

along the chain. Multilevel enforcement relies on the interoperability between **INTERPOL** (via forensic laboratories and the *Project S-Print* monitoring chemical-typographic precursors) and **Europol** (designated as the EU central office under Decision 2005/511/JHA), coordinating cross-border operations and multi-million seizures within the permanent **EMPACT** platform.

- **Systemic Interconnection and the Cybercrime Nexus:** The counterfeiting of means of payment acts as a predicate offense for money laundering and a funding mechanism for terrorism. Financial digitalization has extended the threat toward *cybercrime*, introducing emerging practices of **crypto-counterfeiting and e-commerce fraud**. These developments require constant updates to banking supervision frameworks (the EU **AMLR** package of 2024) and cryptographic market transparency rules (MiCA Regulation) to secure public trust in the co-existence of cash and the digital euro.

# Violation of Union Restrictive Measures

*by Francesco Foccillo*[*]

SUMMARY: I. What Is the Legal Nature of EU Sanctions Within the CFSP? – II. What Strategic Objectives Does the Council Pursue Through Sanctions? – III. Which Subjects Can Be Targeted by EU Restrictive Measures? – IV. Which Subjects Can Be Targeted by EU Restrictive Measures? – V. Which Institutional Tools Regulate the Implementation and Transparency of Sanctions? – VI. How Was the Violation if Sanctions Elevated to the Status of a Tenth "Eurocrime"? – VII. Which Conducts Constitute the Offence and How is it Transposed in Italy? – VIII. What Criminalization Obligations Are Imposed by Directive 2014/62/EU Regarding Currency Counterfeiting? – IX. What is the geopolitical projection of the sanction system toward third and candidate countries?

KEY FINDINGS: Dual legal nature; Targeted approach and proportionality; Elevation to Eurocrime; Italian domestic transposition and corporate liability; Judicial oversight and substantive control.

## I. What Is the Legal Nature of EU Sanctions Within the CFSP?

Restrictive measures, commonly referred to as "sanctions," represent an operational tool of an intrinsically public and EU nature, serving as a core pillar of the **Common Foreign and Security Policy (CFSP)** pursuant to Title V of the Treaty on European Union. The adoption of these instruments does not respond to a purely punitive or retributive logic in the strict sense; rather, it constitutes a coercive, dissuasive, and preventive strategy of a diplomatic and economic nature, designed to react against the violation of peremptory international norms. The European Union deploys sanctions as part of an integrated, multilevel, and global political approach, conceived to act in synergy with political dialogue, bilateral and multilateral diplomatic efforts, and common commercial or financial policies managed by the Brussels institutions.
From a typological standpoint, the sanctions applied by the European Union are divided into three dogmatic macro-categories:

- **Autonomous sanctions:** adopted by the EU on its own initiative whenever the Council deems it necessary to intervene to promote CFSP objectives, even in the absence of international determinations, thereby framing the Union as an independent geopolitical actor;
- **Sanctions in implementation of United Nations resolutions:** adopted by the Union to transpose and execute binding resolutions issued by the UN Security Council under Chapter VII of the UN Charter within the internal market;

[*] Ph.D. Student in Legal Sciences, Member of the Research Staff of the International & European Criminal Law Observatory (IECLO), University of Salerno, Italy.

- **Mixed sanctions:** complex sanction regimes that integrate and combine measures established at the UN level with additional, more stringent, and extensive restrictions autonomously deliberated by the European Union to target specific logistical or financial nodes.

From the perspective of competence allocation and multilevel drafting techniques, they structurally originate from Council decisions adopted unanimously within the framework of the CFSP (pursuant to Article 29 TEU). Subsequently, for aspects that have a direct impact on the economic order and require the limitation of subjective rights within the single market, these decisions are implemented on a material and domestic level through Council regulations adopted by a qualified majority on a joint proposal from the High Representative and the Commission (pursuant to Article 215 TFEU). This procedural decomposition guarantees an immediate, uniform, and directly applicable (*self-executing*) effect for all public and private legal and economic operators acting under EU jurisdiction, without the need for intermediate national transposition acts.

**REFERENCES**

**TEU, Art. 21 and Art. 29**

**Article 21**: "1. The Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law.

The Union shall seek to develop relations and build partnerships with third countries, and international, regional or global organisations which share the principles referred to in the first subparagraph. It shall promote multilateral solutions to common problems, in particular in the framework of the United Nations.

2. The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations, in order to:

(a) safeguard its values, fundamental interests, security, independence and integrity;

(b) consolidate and support democracy, the rule of law, human rights and the principles of international law;

(c) preserve peace, prevent conflicts and strengthen international security, in accordance with the purposes and principles of the United Nations Charter, with the principles of the Helsinki Final Act and with the aims of the Charter of Paris, including those relating to external borders;

(d) foster the sustainable economic, social and environmental development of developing countries, with the primary aim of eradicating poverty;

(e) encourage the integration of all countries into the world economy, including through the progressive abolition of restrictions on international trade;

(f) help develop international measures to preserve and improve the quality of the environment and the sustainable management of global natural resources, in order to ensure sustainable development;

(g) assist populations, countries and regions confronting natural or man-made disasters; and

(h) promote an international system based on stronger multilateral cooperation and good global governance.

3. The Union shall respect the principles and pursue the objectives set out in paragraphs 1 and 2 in the development and implementation of the different areas of the Union's external action covered by this Title and by Part Five of the Treaty on the Functioning of the European Union, and of the external aspects of its other policies.

The Union shall ensure consistency between the different areas of its external action and between these and its other policies. The Council and the Commission, assisted by the High Representative of the Union for Foreign Affairs and Security Policy, shall ensure that consistency and shall cooperate to that effect."

Foundations of sanctions, unanimity, and objectives of the external action of the CFSP

**Article 29:** "The Council shall adopt decisions which shall define the approach of the Union to a particular matter of a geographical or thematic nature. Member States shall ensure that their national policies conform to the Union positions."

**REFERENCES**

**TEU, Art. 31**

"1. Decisions under this Chapter shall be taken by the European Council and the Council acting unanimously, except where this Chapter provides otherwise. The adoption of legislative acts shall be excluded.
When abstaining in a vote, any member of the Council may qualify its abstention by making a formal declaration under the present subparagraph. In that case, it shall not be obliged to apply the decision, but shall accept that the decision commits the Union. In a spirit of mutual solidarity, the Member State concerned shall refrain from any action likely to conflict with or impede Union action based on that decision and the other Member States shall respect its position. If the members of the Council qualifying their abstention in this way represent at least one third of the Member States comprising at least one third of the population of the Union, the decision shall not be adopted.
2. By derogation from the provisions of paragraph 1, the Council shall act by qualified majority:
- when adopting a decision defining a Union action or position on the basis of a decision of the European Council relating to the Union's strategic interests and objectives, as referred to in Article 22(1),
- when adopting a decision defining a Union action or position, on a proposal which the High Representative of the Union for Foreign Affairs and Security Policy has presented following a specific request from the European Council, made on its own initiative or that of the High Representative,
- when adopting any decision implementing a decision defining a Union action or position,
- when appointing a special representative in accordance with Article 33.
If a member of the Council declares that, for vital and stated reasons of national policy, it intends to oppose the adoption of a decision to be taken by qualified majority, a vote shall not be taken. The High Representative will, in close consultation with the Member State involved, search for a solution acceptable to it. If he does not succeed, the Council may, acting by a qualified majority, request that the matter be referred to the European Council for a decision by unanimity.
3. The European Council may unanimously adopt a decision stipulating that the Council shall act by a qualified majority in cases other than those referred to in paragraph 2.
4. Paragraphs 2 and 3 shall not apply to decisions having military or defence implications.
5. For procedural questions, the Council shall act by a majority of its members."

**REFERENCES**

**TFEU, Art. 215**

"1. Where a decision, adopted in accordance with Chapter 2 of Title V of the Treaty on European Union, provides for the interruption or reduction, in part or completely, of economic and financial relations with one or more third countries, the Council, acting by a qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the Commission, shall adopt the necessary measures. It shall inform the European Parliament thereof.
2. Where a decision adopted in accordance with Chapter 2 of Title V of the Treaty on European Union so provides, the Council may adopt restrictive measures under the procedure referred to in paragraph 1 against natural or legal persons and groups or non-State entities.
3. The acts referred to in this Article shall include necessary provisions on legal safeguards."

## II. What Strategic Objectives Does the Council Pursue Through Sanctions?

The imposition of sanctions by the Council is strictly conditioned upon and subordinate to the pursuit and safeguarding of mandatory and constitutionalized objectives, which mirror the supreme values of the EU legal order and the core principles of general

international law. European institutions do not enjoy absolute or unfettered discretion outside the perimeter of the Treaties; they must motivate each sanction regime based on specific subversive or emergency circumstances. First, restrictive measures aim to protect the common security, geopolitical integrity, independence, and fundamental interests of the Union in the face of external threats, asymmetric conflicts, or wars of aggression. Second, they intervene to preserve international peace, prevent the outbreak or deterioration of global and regional armed conflicts, and favor the peaceful resolution of international disputes in conformity with the UN Charter.
Third, restrictive measures play an essential role in promoting, protecting, and consolidating the **Rule of Law**, democratic institutions, human rights, minorities, and fundamental freedoms, targeting in a precise manner the conduct of third-country governments or non-state actors that violate the standards of *jus cogens* or commit international crimes. Finally, sanctions act as a lever to strengthen international security, counter the proliferation of weapons of mass destruction, neutralize the financing of terrorism, and induce a structural and lasting shift in the unlawful conduct or aggressive policies of the targeted subject. Concurrently, they offer a channel for review and revocation of the measures if the conduct of the target aligns with the demands of the international community.

## III. Which Subjects Can Be Targeted by EU Restrictive Measures?

The scope and passive subjectivity of European Union sanctions are structured in an asymmetric, flexible, and targeted manner (**"smart sanctions"**), moving beyond the obsolete logic of comprehensive embargoes against entire territories to selectively hit the nerve centers of criminal, political, or economic power depending on the source of the threat. First, they target **governments of third countries** and their state authorities whenever their external or internal conduct openly violates international treaties or threatens regional stability. Second, sanctions directly hit **corporate entities, public undertakings, financial institutions, and legal persons** that provide the essential economic, technological, industrial, or logistical support to implement and sustain such illicit policies, thereby dismantling the supply chains of strategic or military goods.
Third, the Council directs specific and dynamic restrictive measures toward **non-state groups, networks, militias, or organisations**, including transnational terrorist networks or cartels dedicated to the trafficking of arms and narcotics, striking the underground financial infrastructure that feeds their operations. Finally, sanctions target **natural persons** on a strictly individual basis (such as heads of State, top political figures, oligarchs, industrial magnates, military commanders, and security service agents) directly involved in subversive activities, systemic corruption, human rights violations, or acts of armed aggression. Toward these individuals, the Union's action operates a genuine economic, financial, and personal paralysis, excluding them from the transparent financial circuits of the West and neutralizing their capacity for cross-border influence.

## IV. What Is the Material Content of Sanctions and How Does Proportionality Apply?

In terms of material and prescriptive content, EU restrictive measures are articulated through a plurality of specific material interventions and prohibitions modulated by the Council to ensure maximum effectiveness. These measures encompass:

- The **freezing of capital, funds, bank deposits, and economic resources** belonging to designated persons or entities, which blocks the availability of any financial asset without implying expropriation or the transfer of ownership;
- The absolute prohibition on making financial resources, funds, or assets available, directly or indirectly, to or for the benefit of subjects included in the sanction schedules;
- **Travel restrictions** and bans on entering, transiting through, or staying in the geographical territory and common space of EU Member States;
- **Bans on flying over the airspace** of the EU and on accessing European ports and airports for carriers, aircraft, or vessels flying the flag of or controlled by the sanctioned country;
- Sector-specific **commercial and trade embargoes**, which prohibit the export or import of arms, ammunition, critical technologies, dual-use goods, and industrial services in the energy, transport, aerospace, and oil refining sectors;
- The suspension of visa facilitation provisions for officials, diplomats, and business leaders of the third country, while maintaining access for ordinary citizens.

From the standpoint of constitutional balance, the European Union strictly adopts the technique of "targeted sanctions," structured to hit only those responsible for the unlawful conduct, thereby safeguarding the principle of proportionality under Article 5 TEU. This model is designed to minimize negative externalities and harmful humanitarian or economic consequences for innocent third parties, with specific regard to the **local civilian population** of third countries. The technical design ensures the automatic inclusion of humanitarian carve-out clauses or prior authorization mechanisms by national competent authorities to guarantee the continuity of flows of basic necessities, medicines, food, and medical equipment, ensuring full compliance with international law obligations.

## V. Which Institutional Tools Regulate the Implementation and Transparency of Sanctions?

The management, standardization, and methodological evolution of the common sanction system are rigidly governed by the **"Guidelines on the implementation and evaluation of restrictive measures,"**. This is a strategic and interinstitutional document, originally adopted by the Council of the European Union in 2003 and constantly subject to review, refinement, and updating (specifically in the 2005, 2009, 2012, and 2017 historical editions) to incorporate the evolution of diplomatic practice, the emergence of new cyber or hybrid threats, and the jurisprudential constraints set by the Court of Justice. These guidelines fix standardized legal definitions (e.g., the notion of "funds" or "freezing"), minimum evidentiary criteria for adopting sanctions, binding parameters for monitoring the concrete implementation of measures by the national authorities of the Member States,

and methods for measuring the material impact and macroeconomic effectiveness on targeted subjects.
To support legal certainty, institutional transparency, and the accessibility of this massive and fluid regulatory framework for legal practitioners, magistrates, and global economic operators, the Union formally relies on the **EU Sanctions Map**. This official platform, which stemmed from an innovative initiative of the Estonian Presidency of the Council, offers a digital interface of visual and geographical summary. It allows for real-time consultation of active sanction regimes, the updated list of designated subjects, and the regulatory details of commodity or financial restrictions in force, thereby reducing the risks of inadvertent sanction violations.

## VI. How Was the Violation if Sanctions Elevated to the Status of a Tenth "Eurocrime"?

Historically, the purely administrative or civil nature of sanction enforcement and the fragmentation of national criminal legal systems created deep cracks in the effectiveness of the Union's external action: the exact same conduct of violating or evading CFSP sanctions was considered a serious criminal offence punished with imprisonment in one Member State and a mere administrative infraction subject to a financial criminalty in another. This structural asymmetry generated dangerous phenomena of *forum shopping*, allowing criminal and oligarchic actors to channel illicit financial flows through European jurisdictions endowed with laxer enforcement frameworks, undermining the Rule of Law and common security.
Faced with this geopolitical emergency and the need to ensure a symmetric and inflexible application of economic blocks, the Council of the EU activated the passerelle clause contained in the **third subparagraph of Article 83(1) TFEU**. This norm grants the Council the power to expand the catalogue of **Eurocrimes** by adding other areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of the offences or from a special need to combat them on a common basis.
Through the historic constitutional step of **Council Decision (EU) 2022/2332**, adopted unanimously by the Council on 28 November 2022 after obtaining the consent of the European Parliament, the **violation of Union restrictive measures** was officially elevated to the status of a tenth Eurocrime, entering the second subparagraph of Article 83(1) TFEU. This breakthrough definitively extended the EU's subsidiary criminal competence, providing the essential legal basis for the adoption and issuance of the subsequent **Directive (EU) 2024/1226**, aimed at bindingly harmonizing the definitions of offences, circumvention conducts, and the level of criminal Criminalties applicable across all Member States.

**FRAMEWORK**

**Activation of expansion power** → TFEU Art. 83 para. 1, third subparagraph (developments in crime).

↓

**Constitutional qualification** → Elevation to Eurocrime (Decision (EU) 2322, 2022, *ex* TFEU, Art. 83 para. 1.

↓

**Harmonization via minimum rules** → Directive (EU) 1226, 2024 (obligation of domestic criminalization)

↓

**Transposition into Italian law** → Legislative Decree No. 211, 30 December 2025 (New chapter I-*bis* c.c.)

**FOCUS**

**The Interconnection with the Proceedings of the European Public Prosecutor's Office (EPPO)**

In cases where the violations of EU sanctions and the smuggling of embargoed goods (e.g. dual-use technological components) lead to a concomitant violation of the financial interests of the Union – such as the evasion of common customs duties or cross-border VAT fraud exceeding €10 million – the European Public Prosecutor's Office activates its direct criminal competence, treating the violation of sanctions as a constituent element of PIF crimes.

## VII. Which Conducts Constitute the Offence and How is it Transposed in Italy?

Pursuant to the common dogmatic framework introduced by **Directive (EU) 2024/1226**, Member States are obliged to criminally suppress a mandatory series of material conducts committed intentionally or, in relation to specific conducts involving military goods, with serious negligence. From an objective standpoint, the following actions constitute the offence of violating sanctions:

- The failure to freeze funds, capital, or real estate assets belonging to designated subjects;
- Making economic or financial resources available to or for the benefit of persons or entities inscribed in blocking lists;
- The provision of legal, financial, banking, engineering, or consulting services prohibited by European regulations;
- The import or export of goods subject to a trade ban or embargo, or the trade of dual-use goods without the required ministerial authorizations;
- The knowing violation of travel bans or entry and transit prohibitions within the territory of the Union.

The criminalization of **circumvention conducts** (*circumvention*) assumes an autonomous and innovative importance. Behaviors aimed at hiding, disguising, or concealing the real ownership, beneficial ownership, rights of enjoyment, or control of movable or immovable property constitute a criminal offence. This includes the fraudulent movement of capital to third countries or the use of nominees and fictitious, shielded corporate structures (**"shell companies"**) directed at severing the visible financial link with the sanctioned subject.

In our domestic context, **Italy** has given comprehensive, timely, and strict effect to these Eurocrime protection obligations through **Legislative Decree no. 211 of 30 December 2025** (published in the Official Gazette on 9 January 2026 and officially entering into

force on **24 January 2026**), enacted by virtue of the 2024 European Delegation Law (L. no. 91/2025). This structural reform overcame the old and fragmented sanctioning system based on Legislative Decree no. 109/2007 by inserting the unprecedented **Chapter I-bis**, rubricked *"Offences against the foreign policy and common security of the European Union"* (Articles 264-bis ss. c.c.), into Book II of the Italian Criminal Code. Decree no. 211/2025 punishes offences of violation and circumvention of sanctions with imprisonment for up to five years. It has also introduced a fundamental expansion at the corporate level, placing these offences among the predicate offences of **corporate administrative liability under Legislative Decree no. 231/2001**. This exposes involved companies to heavy financial fines and the interdictive sanction of business suspension, in addition to mandating the compulsory confiscation of the profit or proceeds of the crime.

**REFERENCES**

**Italian Legal Framework Excerpts**

- **For the criminalization of material violations (Freezing of assets and travel bans).**

Article 264-ter of the Italian Criminal Code (introduced by Legislative Decree no. 211/2025): "Punishes with imprisonment from two to five years and a fine anyone who violates the restrictive measures of the European Union relating to the freezing of funds and economic resources or to travel and entry bans."

- **For the punishment of evasive conducts (Circumvention and corporate shields).**

Article 264-*quinquies* of the Italian Criminal Code (introduced by Legislative Decree no. 211/2025): "Punishes with imprisonment from one to four years anyone who commits fraudulent acts, uses nominees or shell companies in order to elude or circumvent the application of the restrictive measures of the European Union."

- **For the extension of criminal/administrative liability to corporations.**

Article 25-*septiesdecimo* of Legislative Decree no. 231 of 8 June 2001 (introduced by Legislative Decree no. 211/2025): "Provides for the application of financial fines (up to 1,000 quotas) and interdictive sanctions (including the prohibition from exercising business activities) against the entity or company in whose interest or advantage the offences of violation or circumvention of EU sanctions have been committed."

## VIII. What Criminalization Obligations Are Imposed by Directive 2014/62/EU Regarding Currency Counterfeiting?

The European Parliament and the constitutional case law of the Court of Justice have repeatedly reaffirmed that the macroeconomic effectiveness and political cogency of the sanction strategy can never bypass absolute and intangible respect for the core principles of **due process**, legality, and the Rule of Law, enshrined in Art. 47 and Art. 48 of the Charter of Fundamental Rights of the EU. To guarantee the democratic legitimacy of the sanction regime and prevent institutional arbitrariness, the EU legal order mandates the adoption of rigorous, objective, documented, and transparent evidentiary criteria for both initial listing (*listing*) and the removal of names from restrictive schedules (*delisting*).
Private subjects subjected to sanctions must have timely notification channels, the fundamental right to be heard by institutions before the reconfirmation of the measure, and the power to submit motivated requests for administrative review directly to the Council of the European Union. From the standpoint of judicial legality oversight, the full and effective exercise of the **right to an effective judicial remedy** must be guaranteed, allowing for the formal challenging of designation acts before the General

Court and the Court of Justice in Luxembourg. This ensures that European judges can operate a thorough judicial review of both the formal correctness of the procedure and the material and documentary merits of the evidence adduced by the Council.

**CASE STUDY**

**Leading Cases of the Court of Justice**

**The Foundational Constitutional Ruling: Commission v. Council, 2005:** A landmark judgment in which the Court of Justice established the existence of implied criminal competences of the Community whenever the criminal harmonization of Member States proves indispensable to ensure the full effectiveness of European protective rules and policies, tracing the dogmatic line that led to the current model under Article 83 TFEU.

**Judicial Reviewability of the CFSP: PJSC Rosneft Oil Company v Her Majesty's Treasury and Others, 2017:** The Court of Justice definitively reaffirmed its full jurisdiction and competence to give preliminary rulings on the validity of restrictive measures adopted within the framework of the CFSP against natural or legal persons, clarifying that the rule of law excludes safe havens and that national courts can refer matters to Luxembourg to safeguard the right to an effective remedy.

**Corporate Circumvention in Public Procurement: Opera Laboratori Fiorentini, 2026**: A core ruling delivered on the interpretation of Regulation (EU) no. 833/2014 concerning sanctions against Russia. The Court provided clarifications of significant systemic impact, decreeing that the ban on the continuation and award of public contracts and concessions to Russian subjects applies if the economic operator acts "on behalf or at the direction" of the State or targeted entities. The Court enshrined the primacy of substantive economic control over abstract legal form to neutralize evasion and cross-border circumvention.

**FOCUS**

**The EU Global Human Rights Sanctions Regime (GHRSR)**

**The EU Global Human Rights Sanctions Regime (GHRSR)**

The EU regulatory framework, adopted on December 7, 2020, with a major geopolitical impact inspired by the US *Magnitsky Act* model, implements the **Global Human Rights Sanctions Regime (GHRSR)**. This horizontal protection tool empowers the Union to impose targeted sanctions (asset freezes and travel bans) against natural persons, legal entities, and state or non-state bodies responsible for, involved in, or associated with serious human rights violations and abuses, **regardless of the geographical location where such crimes were perpetrated or the domestic immunity of the subjects involved**. The GHRSR is characterized by a strong transnational and cross-border nature, and articulates itself across three levels of objective protection:

- **Core international crimes**, with specific reference to the conducts of genocide, crimes against humanity, and war crimes that wound the global conscience;
- Serious, systematic violations of fundamental human rights, such as acts of torture, inhuman, cruel, or degrading treatment, reduction to slavery, extrajudicial, summary, or arbitrary executions, the practice of enforced disappearances, and arbitrary arrests or detentions;
- Widespread and organised abuses against internationally protected interests, which include **trafficking in human beings**, systematic violations perpetrated by migrant smugglers, sexual and gender-based violence as a weapon of political conflict, and the violent suppression of the freedom of peaceful assembly, association, expression, press, or religion.

While excluding pure financial corruption offences from its scope (which are governed by parallel sanction regimes), the GHRSR represents an essential safeguard that reinforces the EU's role as a global actor and enables the export of the EU *acquis* on transnational crimes within the framework of foreign policy and commercial relations with third countries.

## IX. What is the geopolitical projection of the sanction system toward third and candidate countries?

Although formal and executive competence for the application and enforcement of sanctions is firmly vested in the administrative and judicial authorities of the individual Member States, the real political, dissuasive, and economic leverage of the sanction regime rests on its geographical extension, its territorial impenetrability, and international coordination with allied blocs. The European Union activates a complex and extensive network of multilevel geopolitical cooperation, systematically inviting **candidate countries for EU accession** (such as Albania, Bosnia and Herzegovina, Georgia, North Macedonia, Moldova, Montenegro, Serbia, Turkey, and Ukraine), historical commercial partners of the **European Free Trade Association (EFTA)**, and extra-EU Member States of the **European Economic Area (EEA)** (Iceland, Liechtenstein, and Norway) to mirror its restrictive measures.
The alignment with and timely domestic transposition of European sanctions against *cross-border crimes* and transnational threats do not constitute a mere diplomatic option or international courtesy; on the contrary, they serve as a binding parameter, an indicator of political reliability, and a determining element for the overall assessment of the integration and formal accession process to the Union, as well as for developing bilateral commercial relations within the framework of the **European Neighbourhood Policy (ENP)**. This mechanism allows the effectiveness of sanctions to extend far beyond the material borders of the 27 Member States, suffocating external channels of laundering and circumvention.

**FOCUS**

**The Geopolitical and Operational Practice of the Sanction Regime**

- **The Sanction Model against the Russian Federation (2014-2026):** Introduced in response to the illegal annexation of Crimea and Sevastopol in 2014 and intensified following the military aggression against Ukraine, these include **diplomatic measures** (cancellation of summits, interruption of visa facilitation for officials and diplomats), **individual measures** (asset freezes), **media restrictions** (suspension of broadcasting activities of *Sputnik* and *Russia Today* within the European space to counter information manipulation), and **massive sector-specific economic sanctions** (blocking the **SWIFT** system for Russian banking institutions, prohibiting transactions with the Central Bank, restrictions on dual-use goods, and freezing technological exports).
- **The Sanction Model against the Belarus Regime:** Originally activated in 2004 to Criminalize the unresolved disappearances of opposition figures and journalists, the sanction regime was extended in response to the violent repression of peaceful demonstrations following the non-free and unfair presidential elections of August 2020, and subsequently aggravated due to the country's logistical and military involvement in the invasion of Ukraine. Restrictions are articulated through a strict arms embargo (introduced in 2011), individual sanctions against the political leadership, sector-specific trade restrictions, and blocking access to SWIFT. This framework is complemented by the Union's coordinated response to so-called **hybrid attacks** launched along European external borders, characterized by the political instrumentalization of vulnerable migrant flows by the Minsk regime, countered by the EU through emergency financial support and the enhancement of mechanisms to prevent human trafficking.

## X. Key Findings

- **Dual Legal Nature:** EU sanctions are preventive foreign policy tools (CFSP) rather than purely punitive measures. They originate as unanimous Council Decisions and are made directly applicable across the single market through Council Regulations.
- **Targeted Approach and Proportionality:** The EU avoids total embargoes in favour of targeted measures against specific governments, entities, and individuals (asset freezes, travel bans, trade restrictions). Broad proportionality is kept through mandatory humanitarian carve-outs.
- **Elevation to Eurocrime:** To eliminate fragmented national enforcement and prevent circumvention, Council Decision (EU) 2022/2332 added sanction violations to Art. 83(1) TFEU, paving the way for the harmonization criminal offences and Criminalties across all Member States.
- **Italian Domestic Transposition and Corporate Liability:** Transposed via Legislative Decree No. 211/2025, Italy introduced Arts. 264-*bis et seq*. into its Criminal Code, punishing violations and evasive acts with up to 5 years' imprisonment. It also extended corporate administrative liability to cover these offences.
- **Judicial Oversight and Substantive Control:** Listing decisions remain subject to fundamental rights protections and full judicial review by the CJEU. Recent jurisprudence establishes that substantive economic control prevails over legal formalities to strip away shell-company protections and prevent circumvention.