BETKONEXT
Better Knowledge for the Next Generations

Deliverable 3.3

Working paper

Competent authorities and EU's financial interests: new challenges, case-studies, and examples of good practice

Elisabetta Tatì, Camilla Ramotti, Krystyna Bakhtina, Oscar Capdferro Villagrasa, Maciej Serowaniec [eds.]

Under the direction of Aldo Sandulli, Maurizio Bellacosa, Emanuele Birritteri Maurizia De Bellis, Filippo Dinacci, Antonio Gullo, Cristina Fasone, Alessandro Nato, Michele Panzavolta, Rossella Sabia, Marta Simoncini

The BETKONEXT project (Grant Agreement (GA) No: EU-101140537) was co-funded by the EU, under the Union Anti-Fraud Programme (EUAF-2023-TRAI)

DISCLAIMER

The BETKONEXT Project (Grant Agreement (GA) No: EU-101140537) was co-funded by the EU under the Union Anti-Fraud Programme (EUAF-2023-TRAI). The information in this Deliverable reflects only the authors' views, and the European Union is not liable for any use that may be made of the information contained therein.

DISSEMINATION LEVEL

Public

Project:	BETKONEXT– Better Knowledge for Next Generations
GA:	101140537
UAF Programme:	EUAF-2023-TRAI
Funding Scheme:	Co-funding

Working Paper

Competent authorities and EU's financial interests: new challenges, case-studies, and examples of good practice

Work Package 3 - Deliverable 3.3

Due date:	30.11.2025
Submission date:	28.11.2025
Lead beneficiary:	LUISS University
Editors:	Elisabetta Tatì, Camilla Ramotti, Krystyna Bakhtina, Oscar Capdeferro Villagrasa, Maciej Serowaniec
Supervision and Coordination:	Prof. Aldo Sandulli, Prof. Maurizio Bellacosa, Dr. Emanuele Birritteri, Prof. Maurizia De Bellis, Prof. Filippo Dinacci, Prof. Antonio Gullo, Prof. Cristina Fasone, Prof. Alessandro Nato, Prof. Michele Panzavolta, Dr. Rossella Sabia, Prof. Marta Simoncini

ACKNOWLEDGEMENTS

The scientific coordinators of the D3.3 Deliverable project were Professors Aldo Sandulli, Maurizio Bellacosa, Maurizia De Bellis, Filippo Dinacci, Antonio Gullo, Cristina Fasone, Alessandro Nato, Michele Panzavolta, Rossella Sabia, and Marta Simoncini. The editors were Elisabetta Tatì, Camilla Ramotti, Krystyna Bakhtina, Oscar Capdeferro Villagrasa, and Maciej Serowaniec. Each Member State enlisted the collaboration of several researchers and academic experts. The introductory sections were authored by Professors Alessandro Nato, Maurizia De Bellis, Maciej Serowaniec and Drs Alessandro Gerardi Virgili, Krystyna Bakhtina and Elisabetta Tatì (under the suggestions of Prof. Filippo Dinacci, Prof. Cristina Fasone, and Prof. Aldo Sandulli). The report on Italy was a collaborative effort involving Major Francesco Coppola and Captain Federico Gragnoli, from *Guardia di Finanza*, Drs Valerio Bontempi, Camilla Ramotti and Elisabetta Tatì, writing from the administrative law perspective, under the supervision of Prof. Aldo Sandulli and Prof. Marta Simoncini. Dr Giorgio Ardizzone produced the work on criminal law under the supervision of Prof. Maurizio Bellacosa, Prof. Antonio Gullo, Dr Rossella Sabia, and Dr Emanuele Birritteri. The Polish report is the work of Prof. Maciej Serowaniec, together with Dr Natalia Daśko, while the Belgian case is based on the work of Dr Krystyna Bakhtina, under the supervision of Prof. Michele Panzavolta and Prof. Aldo Sandulli. The Spanish report was written by Prof. Oscar Capdeferro Villagrasa, together with Dr Noelia Betetos Agrelo.
The research team also wishes to thank the reviewers –Wannes Bellaert, Sveva Del Gatto, Filippo Giunchedi, Daniel Jurewicz, Emanuele La Rosa, Javier Miranzo Díaz, Patrizio Rubechini – for their invaluable suggestions on how to improve the results.

The research groups thanks all the institutions involved in the seminars, workshops and interviews during the last work-packages for their valuable suggestions and indications.

Lastly, the team thanks Prof. Adrian Bedford for the linguistic review of the entire paper.

Summary

Attributions

1. Preliminary remarks	
Par. 1.1	Drs. Tatì and Bakhtina, Profs. Capdeferro Villagrasa and Serowaniec
Par. 1.2	Prof. Nato
Par. 1.3	Prof. De Bellis
Pars. 1.4, 1.4.1	Dr. Gerardi Virgili
2. Italy	
Par. 2.1	Drs. Tatì and Ramotti
Par. 2.1.1	Captain Gragnoli
Par. 2.1.2	Major Coppola
Pars. 2.1.3, 2.1.4	Dr. Ardizzone
Pars. 2.2, 2.2.1	Dr. Tatì
Par. 2.2.2	Dr. Ramotti
Par. 2.2.3	Dr. Bontempi
3. Belgium	
Pars. 3, 3.1, 3.2, 3.3, 3.4, 3.5	Dr. Krystyna Bakhtina
4. Spain	
Pars. 4.1, 4.2.2, 4.2.3, 4.2.3.1, 4.2.4, 4.2.5	Prof. Capdeferro
Par. 4.2, 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.1.3, 4.2.1.4	Dr. Betetos Agrelo
5. Poland	
Pars. 5.1, 5.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.4, 5.4.1, 5.4.2	Prof. Serowaniec
Par. 5.2	Dr. Dasko

1. Preliminary Remarks

1.1. Introduction

In Regulation (EU, Euratom) No 883/2013, the "competent authority" is a designated national or institutional body that cooperates with the European Anti-Fraud Office (OLAF) to investigate fraud and protect the EU's financial interests. In the Regulation, a definition of "competent authority" is currently lacking. In general terms, for an institution to be a competent authority, it should have the legal power to enforce laws in a specific area.

OLAF will provide Member States with assistance from the Commission in organising close and regular cooperation between their competent authorities to coordinate their actions to protect the financial interests of the Union against fraud, in accordance with Art. 1, para. 2, of the Regulation mentioned above. According to the same article (para. 5), competent authorities of the Member States, as well as institutions, bodies, offices, or agencies (which are not competent authorities), may establish administrative arrangements with the Office.

The absence of a definition of the term *"competent authority"* indeed stems from the deliberate caution exercised by the Union legislator; nevertheless, it gives rise to a number of legal and practical difficulties. On the one hand, the Union legislator sought to avoid encroaching upon the sovereign organisational structures of the Member States, as required by the principle of respect for national constitutional identity and institutional autonomy under Article 4(2) of the Treaty on European Union. On the other hand, leaving it entirely to the Member States to determine which authorities are *"competent"* for the purposes of cooperation with OLAF results in a lack of terminological uniformity and creates uncertainty as to which body bears responsibility for operational cooperation and the exchange of information.

From this perspective, the indeterminacy of the concept may be regarded as a deficiency of the Regulation and a factor undermining the effectiveness of cooperation between OLAF and the Member States. In the absence of a harmonised standard, Member States may designate their "competent authorities" in different ways, and in some instances may even leave this competence only partially defined, thereby weakening legal clarity and certainty.

The lack of a definition in Union law becomes particularly problematic in Poland, where the institutional framework responsible for protecting the financial interests of the State and the Union is multilayered, and where the competences of individual institutions – including

the Police, the Internal Security Agency (ABW), the National Revenue Administration (KAS), as well as the internal audit and control bodies – overlap or intersect. In such a setting, an imprecise reference at the EU level gives rise to risks of competence disputes, interpretative ambiguities, and shifting responsibility between authorities. The absence of a clear designation may also lead to the fragmentation of cooperation with OLAF, with different authorities exchanging information in an uncoordinated manner, thereby diminishing the effectiveness of investigations into financial irregularities and fraud.

Another signal that the notion of "competent authority" does not overlap perfectly with each actor involved in the governance (nor with the Anti-fraud coordination service, so called AFCOS), is Article 8 of the Regulation of 2013 on the duty to inform OLAF, according to which the institutions, bodies, offices, and agencies and, in so far as their national law allows, the competent authorities of the Member States must, at the request of the OLAF or on their own initiative, transmit to OLAF any document or information they hold which relates to an ongoing investigation by OLAF and any other document or information considered pertinent which they hold relating to the fight against fraud, corruption and any other illegal activity affecting the financial interests of the Union.

In any case, all these authorities are crucial for implementing anti-fraud measures, exchanging information, and assisting OLAF in its investigations both within the EU and with third countries. However, the variance across Member States, as seen in previous working papers, is high, as each country has its own peculiarities regarding the actors involved in the fight against irregularities and fraud to the detriment of the EU's financial interests.

A key part of this structure is, therefore, the Anti-Fraud Coordination Service (AFCOS), which is established in every Member State to facilitate this cooperation. At least, this seems to have been the intent of the Regulation. In fact, according to recital 10 of the Regulation, OLAF's operational efficiency depends heavily on cooperation with the Member States. Consequently, Member States need to identify their competent authorities that can provide OLAF with the assistance needed to perform its duties. In cases where a Member State has not set up a specialist department at national level with the task of coordinating the protection of the financial interests of the Union and the fight against fraud, a service (the anti-fraud coordination service) should be designated to facilitate effective cooperation and exchange of information with OLAF.

Only in some countries, however, can the AFCOS be considered a competent authority (and the principal one), especially where there were no pre-existing structures for the protection of the EU's financial interests (for example, before the country joined the EU). This is, for example, the case of Romania.

In other cases, the AFCOS is essentially a coordination module (without legal personality), considering the great variety of competent authorities typically involved in the protection of financial interests and the specificities of the sectors. In this sense, the NRRP anti-fraud network established in Italy is evidence of this complexity (see below).

Similarly, in Belgium, the AFCOS operates under a cooperation agreement among the federal State, the Communities, and the Regions. Embedded within the Federal Public Service Economy, it acts as the national contact point for OLAF, coordinating communication and support among the authorities responsible for protecting the EU's financial interests. This setup highlights that, albeit not a single competent authority, the Belgian AFCOS plays a central coordinating role in practice.

Whereas in the previous working papers the research group kicked off by recognising the primary role of AFCOSes, in light of future reforms and perspectives, here the report starts by prioritising the "competent authority", from which the role of AFCOSes also descends.

The working paper centres on the four countries involved in the comparative study. For each national context, real cases and concrete data on fraud schemes are presented, for example, on the revenue side (i.e., Value Added Tax, VAT) and on the expenditure side (i.e., Common Agricultural Policy, CAP, or Recovery and Resilience Facility, RRF).

Some relevant competent authorities have been involved in previous events over the past few months in four different countries. Some members will describe concrete, real-case scenarios, and their work in action in the first person. In other cases, the research group – national units collected the results of the meetings with the institutions, and here, in this report, they describe the main results.

The description will highlight fraudulent schemes. Special attention is paid to the selection and description of cases and fraud schemes in the digital and green sectors (for example, frauds in e-commerce involving EU funds; frauds involving electric bikes, etc.) and to transnational relevance.

Where it was difficult to identify a specific case, the units decided to illustrate a relevant fraud scheme in the country using aggregate data.

The description of real cases and fraud schemes is also an opportunity to outline the procedures (controls, inspections, sanctions, etc.) followed by the competent authorities.

It is, in fact, clear from the previous working papers that each national system has not only its institutional peculiarities, but also administrative law and criminal law traditions.

Hence, in conclusion, what are the objects of the comparative analysis in this working paper, after the presentation of the fraud case and/or the fraud scheme where the main competent authorities are involved?

According to the evidence from the last project events and activities (Torun, Rome, Barcelona, and Bruxelles), the following list shows some of the hottest topics that can be the object of comparison, here as well as in the future:

- the role and regulation of Tax Representatives across countries, for the VAT cases
- the notion and applicability of the confiscation of assets, as a preventive measure to avoid the recovery of funds unduly spent
- how subcontracting is regulated, especially when EU projects are involved (more in general, the risks associated with operations that involve the public procurement market)
- how cost reimbursement options (flat rates, unit costs, lump sums) can be implemented in the country, especially in view of the next MFF, and how they can balance simplification and control at the same time
- Enforcement tools (i.e. sanctions, police intervention) when administrative investigations are carried on and their coordination with criminal procedings
- adoption of risk-oriented tools and the identification of sensitive targets by the police forces and administrations (by FIUs, for example) in view of the monitoring and control of the incidence of financial crimes
- Notion and operability of specific typologies of irregularities and crimes: false information; false guarantees, for example, through insurance companies and the financial market; conflicts of interests; corruption
- Shared notions of suspected and/or suspicious fraud and serious irregularities

For each case, the units not only describe the cases and comment on the relevant legal solutions and tools, but also highlight possible lessons learnt and/or best practices.

For example, from the dialogue with institutions, what emerged was the usefulness of:

- the exploitation of databases and AI-based tools
- administrative cooperation, MOU, networking
- administrative preventive measures: the speed and celerity in the identification of irregularity and fraud through investigation and the freezing of funds before the beginning of a judicial procedure (this allows the reallocation of funds to eligible individuals and to avoid the long and unsatisfactory phase of the recovery of funds unduly spent)
- legislative intervention or soft law interventions (administrative circulars, guidelines)
- The role of whistleblowing mechanisms

These elements serve as points of comparison in the report.

In fact, it must be remembered that fraud schemes today are cross-border within the EU. They are of supranational importance for the integration of the Single Market.

Consequently, it is of great interest to better understand how equivalent actors, such as competent authorities, face similar problems in different national legal systems.

A European Law part will anticipate the comparative analysis, in addition to these practical premises, on the way in which the working paper is built.

In the subsequent subsections, three “umbrella” topics have been identified for introduction by the research group.

First of all, the discussion around the new EU anti-fraud policy and governance is ongoing. It is important to add a preliminary section here to illustrate the next funding period's resources and the expected functioning of the new programmes, in light of lessons learnt from the RRF and the new economic governance.

Secondly, the research group thought it would be useful, before entering each national case study, to provide an overview of the powers Olaf holds to carry out its investigations, mainly inspection powers. The paradox of Regulation 883/2013 is that it refers generically to the national competent authorities, which retain all their powers, but it does not provide OLAF with sufficient legal powers to enforce laws in the specific area of its operations.

Thirdly, the new functioning of the EPPO requires, as is well known, an additional effort to coordinate OLAF activities. Can OLAF be considered a "competent authority" in relation to EPPO, similarly to what happens between OLAF and national institutions? In this regard, one hot topic is the role of complementary investigations between the two institutions. They can be considered a privileged point of observation for the synergies between the two and the identity of OLAF, also with the possibility of understanding where EPPO cannot operate and where, on the contrary, OLAF will be key actor in the future (such as with controls on the RRF, based on a cost-benefit analysis, that do not integrate hypothesis of frauds and crimes, but only irregularities).

1.2. Towards the new EU governance for the protection of the financial interests and budget architecture

The protection of the financial interests of the European Union (EU) is a key principle of European integration, enshrined in Articles 310, 317, and 325 of the TFEU. This principle translates into shared responsibility between the Union and the Member States, which must cooperate to prevent and combat fraud and irregularities affecting the European budget. However, the current context has highlighted the need for a radical rethink of anti-fraud governance and the budgetary architecture. The expansion of the 2021-2027 multiannual financial framework to €1,200.6 billion and the implementation of Next Generation EU, with a budget of €750 billion, have significantly increased exposure to the risk of fraud.

Added to this are increasingly sophisticated threats, such as transnational fraud, organised crime, and the use of advanced technologies such as artificial intelligence, cryptocurrencies, and encrypted communications, which have made detection and enforcement mechanisms more complex. Against this backdrop, the European Commission has launched a strategic review process with the White Paper on the review of the anti-fraud architecture (COM(2025) 546), which aims to integrate this reform into the next multiannual financial framework.

The EU Anti-Fraud Architecture: Structure, Actors, and Challenges

The current structure of the European Union's anti-fraud architecture comprises a number of bodies and instruments, governed by primary and secondary legislation, that aim to ensure the implementation of the obligations arising from Articles 310 and 325 TFEU on the protection of the Union's financial interests. The European Anti-Fraud Office (OLAF), established by Commission Decision 1999/352/EC and currently governed by Regulation (EU, Euratom) No. 883/2013, exercises independent administrative investigative powers for the purpose of preventing, detecting, and combating fraud, corruption, and other illegal activities affecting the Union budget, in both the expenditure and revenue sectors. OLAF is the Commission's main service for defining and implementing anti-fraud policy, operating in accordance with the procedural guarantees and powers conferred by Union financial rules.

Starting in 2021, the establishment of the European Public Prosecutor's Office (EPPO) introduced an element of discontinuity into the system, granting this body direct jurisdiction in criminal matters for crimes affecting the financial interests of the Union, in accordance with Directive (EU) 2017/1371 (the so-called PIF Directive) and Regulation (EU) 2017/1939, which governs enhanced cooperation between participating Member States. The EPPO operates as a single supranational office with powers of investigation and prosecution before national courts, representing the first example of a European authority with direct powers in the field of law enforcement. Alongside these actors, Eurojust and Europol provide coordination and operational support to the judicial and police authorities of the Member States. At the same time, the European Court of Auditors, pursuant to Articles 285 et seq. TFEU, exercises external control over the regularity and legality of the Union's financial operations.

Despite regulatory and institutional consolidation, current governance presents structural challenges. The fragmentation of responsibilities and overlaps between administrative and criminal investigations lead to operational inefficiencies, exacerbated by incomplete digitisation and limited capacity to recover funds, particularly for traditional own resources (customs duties) and VAT. Furthermore, reporting on anti-fraud activities is characterised by heterogeneity and a lack of common indicators, hindering the construction of an integrated accountability framework. The PIF 2024 Report (COM(2025) 426) confirms these critical issues, highlighting that, despite the increase in investigations launched, recovery rates remain modest, and the time taken to complete procedures is excessively long, thus

compromising the effectiveness of the principle of sound financial management enshrined in Article 317 TFEU.

The EU Anti-Fraud Reform: Digitalization, Coordination, and Financial Resilience

The proposal to revise the anti-fraud architecture, outlined in White Paper COM(2025) 546, is based on a systemic approach aimed at ensuring full implementation of the obligations arising from Articles 310 and 325 TFEU, as well as strengthening the principle of sound financial management enshrined in the Union's Financial Regulation. From this perspective, the first objective is to consolidate the complementarity between criminal and administrative investigations by formalising operational protocols governing OLAF's complementary investigations in support of the EPPO, in accordance with Article 101 of Regulation (EU) 2017/1939. This coordination aims to avoid duplication and ensure the effectiveness of precautionary and recovery measures, while respecting the competences of the various bodies.

The second strategic axis is digitisation, which is considered a structural element of the reform. The mandatory submission of data to the Arachne+ platform from January 1, 2028, together with enhancements to the EDES early detection system, responds to the need to strengthen ex-ante controls and detect anomalies. Interoperability with tools such as E-CODEX and ECRIS, as provided for in Regulation (EU) 2023/2844, is a prerequisite for effective cross-border judicial cooperation. The use of artificial intelligence technologies for predictive data analysis, while representing significant progress, must comply with Regulation (EU) 2024/1689 on AI and the provisions of Regulation (EU) 2016/679 on the protection of personal data, to ensure respect for fundamental rights and procedural safeguards. This framework is part of the reform of the Union's budget architecture for the 2028–2034 period, outlined by the European Commission in the MFF (Multiannual Financial Framework) package. It is not limited to an accounting revision but introduces a regulatory and organisational structure consistent with the principles of transparency, efficiency, and protection of financial interests enshrined in Articles 310 and 325 TFEU. The proposal, which provides for an overall allocation of approximately €1.98 trillion (equal to 1.26% of EU GNI), is characterised by the simplification of programs, greater flexibility in reallocating resources, and the integration of extraordinary crisis instruments, in implementation of the principle of proportionality and the need to ensure the Union's financial resilience. From a legal perspective, the new architecture introduces national and regional partnership plans, which consolidate fourteen funds totalling

€865 billion, with the aim of strengthening coherence between the Union's priorities and those of the Member States. This mechanism is based on strict conditionality obligations, particularly regarding compliance with the rule of law under Regulation (EU, Euratom) 2020/2092, and adherence to anti-fraud and anti-corruption rules. Breach of these obligations entails the suspension of payments and the activation of exclusion procedures from funding, in line with the EDES (Early Detection and Exclusion System), enhanced by the 2024 Financial Regulation.

An innovative element is the adoption of a single performance framework, which reduces the number of indicators from 5,000 to 900 and introduces an integrated annual report on budget management and performance, in line with the principle of accountability. This framework is directly linked to anti-fraud governance, imposing harmonised reporting obligations on authorising officers and Member States and requiring the use of interoperable digital tools, such as the Arachne+ platform, which will become mandatory from 2028. Furthermore, the centralised database of EU fund beneficiaries, envisaged by the new Financial Regulation, constitutes an essential legal safeguard to ensure transparency and prevent conflicts of interest.

From Fragmented Governance to Systemic Integration: The EU's Anti-Fraud Paradigm Shift

The reform also introduces new own resources (ETS, CBAM, electronic waste contribution, tobacco excise duties, corporate resource), which require strengthened customs and tax controls. In this context, the future EU Customs Authority, as proposed in Regulation COM(2023) 258, will perform risk management and real-time analysis of trade flows, integrating activities to prevent and detect customs fraud. Similarly, the Anti-Money Laundering Authority (AMLA) established by Regulation (EU) 2024/1620 and operational from 2028, will ensure direct supervision in the field of anti-money laundering and counter-terrorist financing, with sanctioning powers that are proportionate and compliant with procedural safeguards.

The link between the new budget architecture and anti-fraud governance thus results in an integrated regulatory system that combines financial flexibility tools with mechanisms of legal control and conditionality. The digitalisation of processes, the harmonisation of rules, and strengthened cooperation between OLAF, EPPO, and national authorities constitute the pillars

of a model aimed at ensuring the effectiveness of protecting the Union's financial interests, in implementation of the principle of legality and the value of the rule of law enshrined in Article 2 TEU.

Another innovative element is the establishment of new entities vested with regulatory and sanctioning powers. AMLA established by Regulation (EU) 2024/1620 and set to become fully operational in 2028, will exercise direct supervisory powers over financial operators and may impose pecuniary sanctions, in accordance with the principle of proportionality and in compliance with the Union's procedural guarantees. Similarly, the future EU Customs Authority, envisaged in the customs reform package (COM(2023) 258), will play a central role in risk management and border controls through the creation of a digital customs centre that will ensure real-time analysis of trade flows in conformity with the provisions of the Union Customs Code. The comparison between the current anti-fraud architecture and the model outlined by the European Commission highlights a systemic paradigm shift. The existing framework, despite being based on primary and secondary legislation that assigns specific competences to Union bodies and Member States, is characterised by fragmented governance, where responsibility for preventing and combating fraud largely rests with national authorities, in accordance with the principle of sincere cooperation under Article 4(3) TEU. The reform proposal, set out in the White Paper COM(2025) 546, instead aims to establish an integrated system, based on operational synergies and governance oriented towards results, in compliance with the principle of sound financial management enshrined in Article 317 TFEU. In this context, digitalisation is designated as a structural element of the new architecture. Whereas under the current regime the use of IT tools is limited to platforms such as IMS and OWNRES, the reform introduces the legal obligation to submit data to Arachne+ as of 2028, together with the enhancement of the Early Detection and Exclusion System (EDES) and interoperability with digital infrastructures such as E-CODEX and ECRIS, as provided for by Regulation (EU) 2023/2844. The use of artificial intelligence technologies for predictive data analysis, while representing a significant advancement, must comply with the requirements of Regulation (EU) 2024/1689 on AI and the provisions of Regulation (EU) 2016/679 on personal data protection, to ensure respect for fundamental rights and procedural safeguards. The process of recovering unduly paid amounts, currently governed by the Financial Regulation and largely entrusted to Member States, is marked by slowness and inefficiency. The reform provides for the introduction of accelerated procedures and early precautionary measures, closely coordinated

with EPPO's criminal investigations and OLAF's administrative investigations, in implementation of the principle of effectiveness in protecting the Union's financial interests. Similarly, reporting, currently fragmented and lacking uniform indicators, will be harmonised through the adoption of common parameters and the integration of data into the PIF Report, to ensure transparency and accountability, in compliance with the reporting obligations laid down in the Financial Regulation.

The data contained in the 2024 PIF Report (COM(2025) 426) confirm the need for this revision: in the reference year, 13,589 irregularities were reported for a total amount of €1.84 billion (+19.5% compared to 2023), of which 1,364 confirmed fraud cases accounted for €548.8 million (+138.7%). OLAF concluded 246 investigations, issuing 301 recommendations for a total of €871.5 million in recommended recoveries, while EPPO initiated 1,504 investigations for an estimated damage of €13.07 billion. These figures show that, although the current system is effective in terms of detection, it does not ensure timely recovery of resources nor adequate preventive capacity, resulting in a compromise of the effectiveness of the principle of protecting the Union's financial interests.

Anti-Fraud Governance as a Pillar of EU Legitimacy and Rule of Law

The new governance for the protection of the Union's financial interests and the reform of the budget architecture cannot be classified as mere technical or administrative measures, but rather as a systemic revision that affects fundamental principles of the European legal order. It falls within the scope of the obligations arising from Articles 310 and 325 TFEU, which require compliance with the principle of sound financial management and the fight against fraud, as shared responsibilities between the Union and the Member States. The reform therefore assumes a constitutional dimension within Union law, as it aims to ensure the effectiveness of the protection of financial interests through appropriate and proportionate instruments, in accordance with the principle of legality and respect for the competences conferred.

The perspectives outlined in the White Paper COM(2025) 546 and in the Justice Programme (COM(2025) 463) shape a model of anti-fraud governance based on proactivity, digitalisation, and strengthened cooperation between Union bodies and national authorities. This model rests on clear legal foundations: the integration of criminal and administrative investigations, the formalisation of cooperation protocols between OLAF and EPPO, the

obligation to ensure interoperability of IT systems, and the creation of new authorities vested with regulatory and sanctioning powers, such as AMLA and the future EU Customs Authority. These innovations directly affect the implementation of the principle of effectiveness, ensuring that the protection of financial interests does not remain confined to a merely formal dimension but translates into tangible results in terms of prevention, detection, and recovery of resources.

The success of the reform, however, depends on the ability to overcome structural challenges in the legal and organisational spheres. First, data interoperability and process digitalisation must be implemented in compliance with personal data protection rules (Regulation (EU) 2016/679) and the procedural safeguards associated with the use of artificial intelligence (Regulation (EU) 2024/1689). Second, regulatory harmonisation between national legal systems and Union law is an essential condition to avoid disparities in application and ensure uniform protection. Similarly, the speed of recovery procedures and the effectiveness of precautionary measures require adjustments to national legal frameworks in line with the Financial Regulation and the PIF Directive. Lastly, the training of operators and the strengthening of technical and legal skills are prerequisites for the effectiveness of the reform, as they ensure the correct application of the rules and full use of digital tools. Only through an integrated approach, based on the principles of proportionality, transparency, and accountability, can the Union establish an anti-fraud governance system capable of ensuring a resilient budget that complies with the values enshrined in Article 2 TEU. In this way, the reform does not merely respond to contingent needs but constitutes a structural intervention aimed at strengthening the legitimacy and credibility of the Union's action, in line with global challenges and the expectations of European citizens.

1.3. Olaf and its inspection powers

OLAF's functions were originally governed by Regulation no. 1073/1999, later replaced by Regulation no. 883/2013; this last act has later been amended with Regulation no. 2020/2223. However, the legal framework regulating OLAF's powers is complex, as Reg. no. 883/2013 refers in several points to Regulations no. 2988/96 and no. 2185/96.

As for its structure, OLAF is an internal organisation of the Commission, but it has autonomy and operational independence: for example, , according to article 17(3), of Reg. no. 883/2013, «The Director-General shall neither seek nor take instructions from any government

or any institution, body, office or agency in the performance of his or her duties with regard to the opening and carrying-out of external and internal investigations or coordination activities, or to the drafting of reports following such investigations or coordination activities. If the Director-General considers that a measure taken by the Commission calls his or her independence into question, he or she shall immediately inform the Supervisory Committee and shall decide whether to bring an action against the Commission before the CJEU».

The scope of OLAF's action covers the fight against fraud, corruption and any other illegal activity affecting the financial interests of the European Union. Traditionally, from the quantitative point of view, the main areas of intervention of OLAF are the Structural Funds and the Common Agricultural Policy. According to the 2024 OLAF report, the areas where OLF's investigations are those on shared management (with those involving the European Regional Development Fund constituting the highest share), together with concerning the Recovery and Resilience Facility (RRF) funds.

OLAF inspections are divided into two types: internal (in cases in which the activities under investigation are carried out by employees of European institutions), and external (related to the conduct of economic operators in the territory of Member States) (Regulation 883/2013, art. 3 and 4).

The type of powers that can be used by OLAF inspectors include (art. 3, paras. 2 and 3, and art. 4, para. 2):

- controls and spot checks;
- requesting oral and written explanations, including interviews;
- access to all information, documents and data relating to the matter under investigation
- in addition to extracting copies of documents, assume custody of documents or data to ensure that there is no danger of their disappearance
- in the case of internal investigations, the Office shall have the right of immediate and unannounced access to any relevant information and data;
- digital forensic operations (DFO) – ie. the identification, acquisition, imaging, collection, analysis and preservation of digital evidence –, can be conducted, an activity which is ruled under specific internal guidelines (Olaf, *Guidelines on Digital Forensic Procedures for OLAF Staff*, 15 February 2016).

Several substantial and procedural conditions apply to OLAF's inspections.

A substantial condition for the initiation of an investigation (both internal and external) is that there is sufficient suspicion (which may be based on information provided by any third party or on anonymous information) of the existence of fraud, corruption, or other activity detrimental to the financial interests of the EU (Reg. 883/2013, art. 5(1)). The decision to initiate the investigation, as expressly provided for by the Regulation, must take into account the resources available to OLAF and, above all, the proportionality of the measures used.

From a procedural point of view, a decision of the Director-General, whether taken on their own initiative or at the request of an interested state or EU institution, is necessary in order to open an investigation (Reg. 883/2013, art. 5(1)). The Director-General, however, does not himself perform the inspections: he shall give written instructions for how the inspections shall be conducted, which is a task to be performed by the staff on the basis of a specific authorization. The authorization shall both identify the staff in charge and indicate the subject matter and the purpose of the investigation, the legal bases for conducting the investigation and the investigative powers stemming from those bases (Reg. 883/2013, art. 7(2)).

In the case of external investigations, the economic operator has a duty to cooperate, as clarified both in Reg. 883/2013 and by the Court of Justice (Case T-48/16, *Sigma Orionis SA v. Commission*).

As regards cooperation with national authorities, for external investigations there is an obligation for national competent authorities to provide the assistance necessary to carry out inspections (Regulation 883/2013, arts. 3(5), and 7(3)). As clarified at the outset, the Regulation does not specify what the competent authority is. According to recital 10 of Reg. 883/2013, «There is a need for the Member States to identify their competent authorities which are able to provide the Office with the assistance needed in the performance of its duties. In cases where a Member State has not set up a specialist department at national level with the task of coordinating the protection of the financial interests of the Union and the fight against fraud, a service (the anti-fraud coordination service) should be designated to facilitate effective cooperation and exchange of information with the Office». As a result, the Member States 'should' designate a competent authority to coordinate and exchange information with OLAF (however, such need to designate is not framed as a specific obligation in one of the provisions of the Regulation – instead, it is expressed in more vague terms in the recital – , contrary to

what is provided for under other Regulations, such as art. 49 of the Digital Services Act (DSA), which obliges Member States to designate a Digital Services Coordinator).

However, in case the economic operator resists the inspection despite its obligations, according to Reg. 883/2013 the obligation to cooperate includes providing access to its premises or any other areas used for business purposes, so that cooperation from Member States would include not only the 'competent' authority as designated by the States specifically for the purpose of cooperating with OLAF – but also law enforcement authorities as providing assistance could require the use of force, following the required national procedures (Reg. 883/2013, art. 3(6)).

OLAF has the power to conduct investigations, but it does not commit sanctions. At the end of the investigation, it prepares a report, describing the preliminary findings, and recommendations. Those recommendations shall indicate disciplinary, administrative, financial or judicial action to be taken by the institutions, bodies, offices and agencies of the EU and by the competent authorities of the Member States concerned. As clarified in the case law of the Court of Justice[1] and now specifically recognized in the revised OLAF Regulation (Regulation 2020/2223, recital 30), such recommendations have no binding legal effect on the EU or Member States authorities. It is up to the EU institution or to national authorities to decide whether to proceed in taking administrative or judicial action.

1.4. OLAF and the EPPO: Functional autonomy and operational synergy

Within the current European framework for the protection of the Union's financial interests, OLAF and the EPPO are two central actors whose relationship is structurally complementary, while each maintains its functional autonomy. The establishment of the European Public Prosecutor's Office has significantly reshaped the mechanisms for combating fraud affecting the Union budget, but it has not replaced OLAF; rather, it has redefined its role

[1] Case T-193/04, *Hans-Martin Tillack v. Commission*, ECLI:EU:T:2006:292 paras. 67-68, 70, 72; Case T-215/02, *Santiago Gómez-Reino v. Commission*, ECLI:EU:T:2002:251, para. 50; Case T-392/17, *TE v. Commission*, ECLI:EU:T:2018:459; Case T-29/03, *Comunidad Autónoma de Andalucía v. Commission*, ECLI:EU:T:2004:235, para. 40; Case T-309/03, *Manel Camós Grau v. Commission,* ECLI:EU:T:2006:110, paras. 55-58; Case T-4/05, *Guido Strack v. Commission*, ECLI:EU:T:2006:93; Case C-237/06, *P Guido Strack v. Commission*, ECLI:EU:C:2007:156; Case T-289/16, *Inox Mare v. Commission*, ECLI:EU:T:2017:414, para. 28.

within an integrated cooperative system that aims to create an "end-to-end" prosecution cycle by procedurally integrating their respective powers, strengthening the capacity of European bodies to effectively combat crime (Bellacosa, De Bellis, 16; Dianesa, Grozdev, 4). This is the perspective underlying Regulation (EU, Euratom) 2020/2223, which adapted the regulatory framework to the operational needs arising from the EPPO's establishment while maintaining a clear distinction between OLAF's administrative investigative mandate and the EPPO's prosecutorial functions.

Under this framework, the two institutions retain their distinct structural and operational identities. OLAF continues to exercise its mandate as the administrative body responsible for conducting non-criminal investigations; these may conclude with financial, administrative, disciplinary, or judicial recommendations (Juric, 2). The EPPO, which is operational in 24 of the 27 Member States, focuses on establishing criminal liability for offences affecting the Union's financial interests, such as fraud, corruption, and other conduct within the scope of its founding regulation.

Although the two bodies operate at different levels, these competences are fully complementary (Inghelram, 189). The cooperation arrangement concluded in July 2021 – as explicitly envisaged by the 2020 amending regulation – sets out the practical modalities of cooperation, structured along four fundamental lines:

- The structured exchange of information, including reciprocal access to electronic case-management systems, to avoid duplication and ensure traceability of each case;

- Notification and transmission of cases, through which OLAF informs the EPPO of matters falling within OLAF's remit, and the EPPO notifies OLAF of unlawful conduct outside its mandate (including in non-participating Member States);

- Mutual support, which enables OLAF to provide the EPPO with technical and specialised expertise, such as digital forensic analysis or expert testimony);

- Complementary investigations, a mechanism allowing the two bodies to operate in parallel by coordinating administrative and criminal actions.

It is precisely the complementary investigations that constitute the most significant and innovative component of the cooperative system.

1.4.1. Complementary investigations

Complementary investigations are among the most innovative and complex elements of cooperation between OLAF and the EPPO, enabling the two bodies to exercise their respective administrative and criminal competences in a coordinated manner in relation to the same conduct that is detrimental to the Union's financial interests. This mechanism thus performs a bridging function between the two layers of the European anti-fraud system, ensuring that punitive measures and the recovery of financial resources can progress in parallel without interfering with each other (Weyembergh, Brière, 62; Dianese, Grozdev, 4).

The primary objective of such investigations is to ensure a comprehensive public enforcement response to conduct that presents both criminally relevant aspects (within the EPPO's competence) and elements requiring administrative or disciplinary measures (within OLAF's competence). The underlying logic is one of functional bifurcation: the EPPO exercises exclusive authority over criminal investigations concerning offences affecting the EU's financial interests, while OLAF, although unable to intervene in criminal matters, retains the capacity to act on the administrative, inspection, and recovery fronts.

Within this framework, a complementary investigation functions as a mechanism of parallel, rather than subordinate, cooperation that avoids institutional blind spots: the existence of a criminal investigation does not paralyse administrative activity, nor does an administrative inquiry hinder the establishment of criminal liability.

The initiative may originate from either body. The EPPO may formally request that OLAF carry out specific administrative activities to support or complete the criminal investigation. Conversely, OLAF may, after consulting the EPPO, initiate a complementary inquiry on its own initiative where it identifies administrative aspects not covered by the ongoing criminal investigation (Covolo, 210). The requirement of prior consultation, set out in the Regulation, is essential to prevent duplicative or obstructive actions.

In the context of complementary investigations, the two bodies exercise distinct but integrated powers:

- The EPPO retains coercive criminal powers (such as searches, seizures, interceptions, or precautionary measures) aimed at establishing criminal liability;

- OLAF exercises administrative and inspection powers (such as on-the-spot checks, interviews of concerned persons, the collection of documentary evidence, and compliance

checks), aimed at financial recovery, the adoption of administrative or disciplinary measures, and the prevention of future irregularities.

This distinction ensures functional specialisation, prevents overlap, and guarantees that each institution operates within its own legal mandate. The synchronisation of activities between the two investigative EU bodies represents a fundamental added value to the comprehensive approach to protecting the EU budget, introducing what could be described as a new EU "joint investigation mechanism" for safeguarding European taxpayers' money. From a practical perspective, coordination between the two bodies is indispensable for planning investigative actions. This is necessary to ensure that the evidence gathered is fully admissible in criminal proceedings before the national courts of Member States. It requires respecting high standards of data protection, respecting individuals' rights (in particular their right to legal assistance and representation), and complying with the limitations imposed by the information holders (e.g., the Member States) on information shared in the course of such investigations.

Upon receiving OLAF's notification of its intention to launch or continue a complementary investigation, the EPPO – pursuant to Article 12-*quinquies* of Regulation (EU, Euratom) No. 883/2013, as amended – has a fixed period within which it may object to OLAF's initiation of the investigation or the execution of specific investigative acts. As specified in the EPPO–OLAF Operational Agreement of 5 July 2021, and consistent with Article 12-o*cties*, this period is set at 20 working days, during which the EPPO must declare any objection. Should the EPPO exercise this option, it must also inform OLAF without undue delay once the grounds for objection have ceased.

Objections are a safeguard mechanism in criminal investigations, designed to prevent administrative acts from compromising evidence gathering or breaching investigative secrecy. However, the EPPO must communicate without undue delay the cessation of the obstructive grounds, enabling OLAF to resume or complete its activities (De Bellis, 171).

The Regulation does not provide sanctions for delayed or missing declarations of objection or for delays in withdrawing opposition. In such circumstances, once the deadline has expired, any subsequent communication will produce no effect and should not hinder activities already initiated. This regulatory gap may, however, affect the timeliness of OLAF's administrative intervention and thus the recovery of financial resources (Kratsas, 95).

Coser analysis shows that the possibility of EPPO refusing OLAF's cooperation, although permitted by the Regulation, would ultimately result in insufficient protection of the

Union's financial interests. If the EPPO were to decide to act alone and not to authorise a complementary investigation, the resulting inquiry might be partial or incomplete. Certain elements (which do not pertain to criminal aspects but constitute irregularities or administrative non-compliance) could nevertheless jeopardise both the Union's financial interests and the very purpose of the disbursement of funds (Ligeti, Robinson, 219). For this reason, OLAF's contribution must be regarded as essential (Weyembergh, Brière, 70).

Of course, particular attention should be paid to coordinating activities to avoid duplication of investigations. The suspension of OLAF's investigations must be ensured when the EPPO is conducting an investigation into the same facts, especially in the light of the *ne bis in idem* principle (enshrined in Article 50 of the Charter of Fundamental Rights of the EU, Article 54 of the CISA, and Article 4 of Protocol No. 7 to the ECHR). The *ne bis in idem* principle also applies to "administrative sanctions" where the so-called Engel criteria, established in the ECtHR's case law, are met. This requires an assessment of "the legal classification of the offence under national law, the very nature of the offence, and the degree of severity of the penalty that the person concerned risks incurring". If the criminal nature of the sanction is confirmed, administrative sanctions that could be imposed on the basis of OLAF's recommendations may preclude the possibility of subsequently conducting a criminal investigation and may exclude the opportunity to impose and enforce genuine criminal penalties.

To limit the risk of violating the *ne bis in idem* principle, Article 101(2) of the EPPO Regulation provides that, where the EPPO is conducting a criminal investigation, "OLAF shall not open any parallel administrative investigation into the same facts".

Only when interpreted in these terms does the EPPO's veto on OLAF's activities find its justification.

A significant contribution to assessing the actual functioning of the mechanism comes from the OLAF Supervisory Committee, which, in Activity Report C/2025/4091, adopted Opinion No. 1/2024, based on an analysis of the first 70 complementary investigations opened by OLAF since June 2021, 40 of which were already concluded and examined in detail. The Committee acknowledged the professionalism and commitment of both institutions to ensuring the new system's effectiveness. However, it issued two recommendations:

(1) the systematic use of the templates and forms agreed with the EPPO, even in cases where an informal advance notice of opposition has been provided;

(2) incorporation of this practice into the future revision of OLAF's procedural guidelines, with the aim of strengthening transparency and administrative coherence.

The Committee also noted that the EPPO has never formally rejected a proposal for a complementary investigation submitted by OLAF, a fact that may be interpreted as a sign of strong cooperation. According to the Committee, this does not appear to be the result of informal practices intended to predetermine the outcome of the procedure.

2. Italy

2.1. Short introduction: findings from the workshop in Rome, Reparti Speciali della Guardia di Finanza, July 2, 2025

On July 2nd, 2025, a high-level workshop entitled "The protection of the EU's financial interests and new trends in fraud schemes – Cases and good practices from the institutional perspective" was held in Rome at the Reparto T.L.A. dei Reparti Speciali of the Guardia di Finanza, within the framework of the BETKONEXT project (Grant Agreement No. 101140537). The event brought together representatives from national and European institutions – including OLAF, the European Delegated Prosecutor for Italy, the Italian Revenue and Customs Agencies, and the Bank of Italy – to discuss practical experiences and new approaches to preventing and investigating fraud affecting EU resources.

The first panel, "EU resources on the revenue side and transnational challenges", focused on fraud patterns related to VAT and customs duties. The Revenue Agency highlighted the persistence of MTIC/carousel and e-commerce fraud, stressing the importance of cooperation tools such as EUROFISC, Transaction Network Analysis (TNA), and CESOP. The Customs and Monopolies Agency reported cases of false declarations of origin, quality, and value and misuse of simplified procedures (Regime 42, IOSS). At the same time, the Guardia di Finanza presented its operational methodology, combining analytical tools and investigations coordinated with the European Public Prosecutor's Office (EPPO).

The second panel, "EU resources on the expenditure side and the RRF: risk of irregularities and fraud in a cross-border scenario", addressed vulnerabilities in shared and direct management. OLAF shared case studies on Horizon 2020, LIFE+ and Resc-EU projects, showing recurring manipulation of procurement procedures and inflated costs. The Guardia di Finanza highlighted NRRP-related cases (Transumanza, Resilient Crime), revealing organised crime infiltration and large-scale fraud. The Financial Intelligence Unit (FIU Italy) illustrated how Suspicious Transaction Reports (STRs) and AML safeguards help identify fraudulent use of EU and national funds, including schemes involving fake financial guarantees in public procurement.

Discussions throughout the workshop confirmed the importance of: (i) identifying high-risk activities to prioritise control and investigation; (ii) enhancing coordination among national and EU bodies; and (iii) reinforcing both administrative and judicial preventive tools to reduce financial losses and improve recovery prospects.

Thus, first of all, identifying activities with a high risk of illegality is essential to concentrate investigative efforts and control them. Specific tools based on new technologies can adequately serve this purpose. Secondly, what emerged was an often insufficient level of coordination among the institutions involved in anti-fraud governance, from the managing authorities to the so-called "competent" authorities. The NRRP anti-fraud network represents, at least on paper, a response to both reported issues. Thirdly, and closely related to the previous problems, many institutions agreed on the need for preventive measures, not only in terms of administrative remedies during the management phase (i.e., transparency regimes to combat corruption, scanning and analysing seemingly minor irregularities, administrative sanctions) but also in the repression phase, with the intent to reduce damage (freezing economic assets, preventive confiscations). Fourthly, last but not least, timely action in the latter sense of "prevention" can reduce the need for recovery procedures, which normally deplete resources and can impact public budgets.

In the following sub-paragraphs, some real case scenarios will be presented by one of the most influential Italian competent authorities under Regulation (EU) No. 883/2013: the Guardia di Finanza. On one side, the major VAT fraud schemes will be presented, focusing on a case study that illustrates the operational role of the Guardia di Finanza. On the other side, following a similar sketch, fraud schemes in the Common Agricultural Policy (CAP) sector will be presented. On the base of these cases, a theoretical analysis by the Criminal Law perspective will conclude the section.

2.1.1. Brief overview of the MTIC fraud mechanism and operational procedures of the Italian Financial Police ('Guardia di Finanza').

a. The anatomy of MTIC fraud: how it works and its key patterns

MTIC fraud, short for Missing Trader Intra-Community fraud, is a form of Value Added Tax (VAT) fraud that exploits the rules of cross-border trade within the European Union (EU).

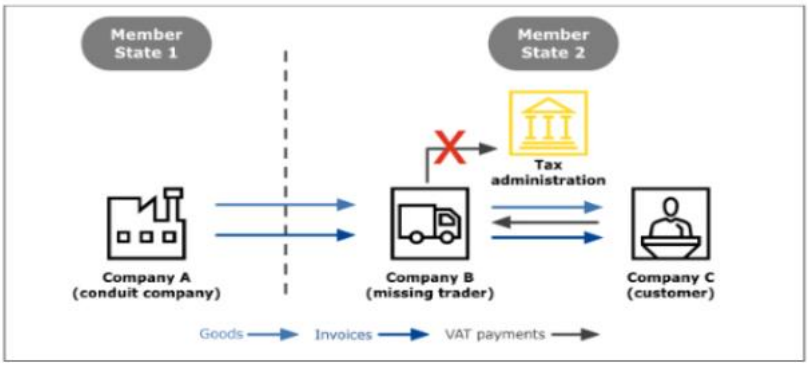
The mechanism relies on the fact that B2B cross-border transactions within the EU use a specific VAT accounting mechanism: the reverse charge, which shifts the VAT-reporting responsibility from the supplier to the customer. In effect, the VAT is neutral for both the supplier (who does not charge the VAT) and the customer (who records both the output VAT and the input VAT).

While this system was designed to simplify VAT collection within the EU, it has created an opportunity for fraudsters. A European company (a missing trader) can "import" goods VAT-free (from another Member State), sell them (often at a discounted price) to another company in its country using the ordinary VAT mechanism, and then disappear without remitting the collected VAT from its domestic customer.

It is worth noting that MTIC fraud can range from simple acquisition fraud to the well-known carousel fraud to the most threatening schemes, which involve several companies across multiple jurisdictions in the EU.

Under its baseline scheme (the so-called acquisition fraud), Company A sells goods to Company B without applying VAT thanks to the reverse charge mechanism. Company B makes a domestic sale to its customer, Company C, and collects VAT. This output VAT is not remitted to the Tax Administration of Member State 2, Company B disappears, and hence, the VAT loss in Member State 2.

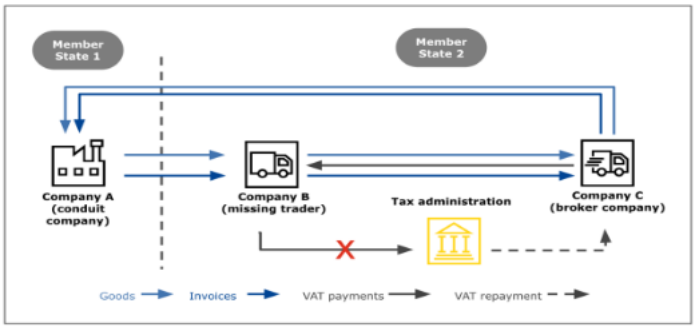
The diagram below helps to understand how MTIC frauds work and the role of each actor involved ["VAT compliance gap due to Missing Trader Intra-Community (MTIC) fraud" final report, Directorate-General for Taxation and Customs Union (European Commission), 2024]:



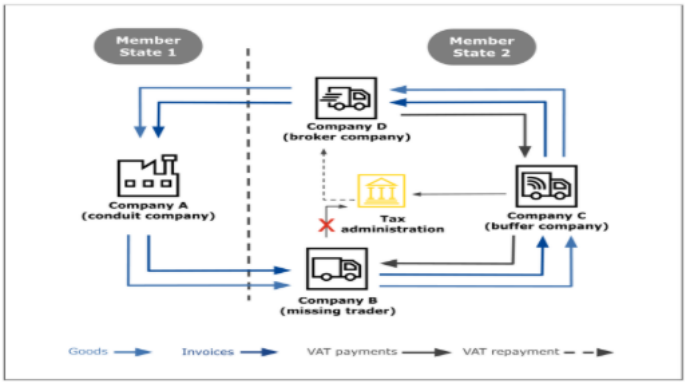
A core element of MTIC fraud is the intentional underselling in the transaction between the missing trader and its customer. The VAT collected and not remitted is used financially to support underpriced sales. Doing so in Member State 2 results in the goods being sold at below-market prices, distorting competition.

As mentioned before, another archetype of MTIC fraud is the carousel scheme, which is widely known and combated by law enforcement agencies across all European Union territory. The main characteristic of this scheme is the "carousel effect", which is the part of the fraud where the same goods (or just the paperwork) keep circulating through the same fraudulent commercial chain, allowing tax criminals to repeatedly defraud the VAT system.

At each loop, the missing trader imports goods from another Member State VAT-free; then, it sells them to its domestic customer, charging VAT but omitting the payment to its tax authority. Eventually, the customer (the broker company) exports the goods to another Member State VAT-free. After the export, the goods are sold to the original country back to the missing trader, and the chain repeats as displayed below ["VAT compliance gap due to Missing Trader Intra-Community (MTIC) fraud", cit.]:

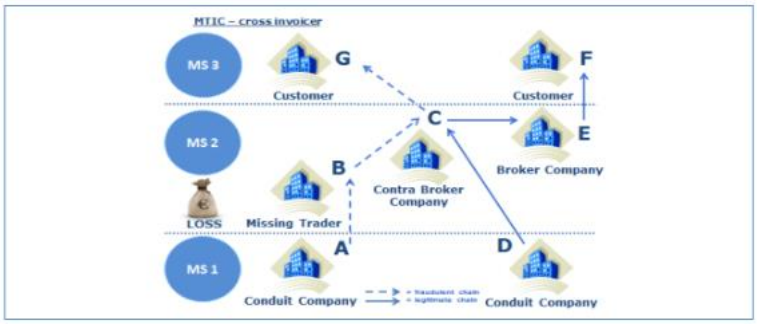


To make the fraud chain look legitimate and harder to detect, fraudsters usually insert another company, known as a "buffer company", between the missing trader and its customer, adding another layer of transactions to disguise the connection between the disappeared trader and the broker. By doing so, buffer companies create the illusion of a normal-looking commercial chain ["VAT compliance gap due to Missing Trader Intra-Community (MTIC) fraud", cit.]:



Another attempt to complicate the detection and the tackling of VAT fraud is the use of contra-trading. The fraudsters set up two parallel commercial chains, the fraudulent one (which contains the missing trader), and the legitimate one. The key trick is that the contra-trader company claims a VAT refund generated from the fraudulent chain, but the connection between the two chains is obscured.

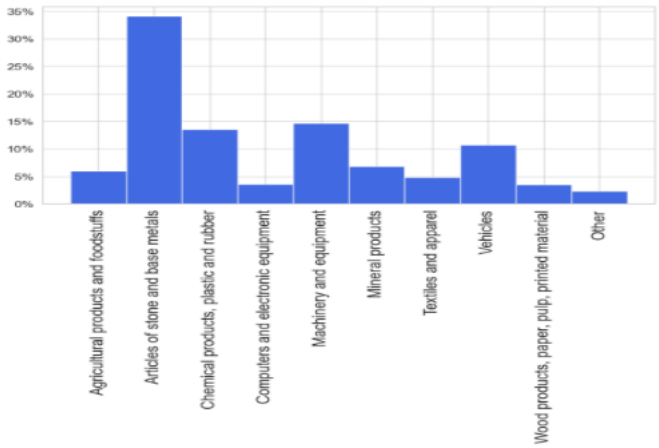
The key steps are as follows: the contra-trading company (C) acquires goods from a domestic missing trader (B) and, at the same time, performs an intra-community acquisition from company D located in Member State 1. Then, the contra-trader makes two sales: an intra-community sale to customer G in Member State 3 and a domestic sale to company E. The VAT that the contra-trader will claim back to its Tax Authority is not the VAT from the goods acquired in the legitimate chain, but it is actually offset by the VAT stolen in the fraudulent chain [The concept of Tax Gaps. Report III: MTIC Fraud Gap Estimation Methodologies. FISCALIS 2020 Tax Gap Project Group, subgroup VAT fraud (FPG/041), November 2018, European Commission]:



Cross-invoicing is another mechanism used to delay the detection of ongoing MTIC fraud. Cross-invoicing schemes, like contra-trading, share the construction of a parallel commercial network used to offset the VAT liabilities generated by the fraudulent chain. In contrast to contra-trading, which uses a legitimate commercial network, the cross-invoicing scheme operates through two fictitious, parallel flows of invoices to avoid detection.

MTIC fraud represents one of the most significant threats to the integrity and stability of the EU's VAT system, costing billions in lost revenue each year. In fact, according to the "*VAT compliance gap due to Missing Trader Intra-Community (MTIC) fraud"* final report published in 2024, the estimated forgone revenue in the EU from MTIC fraud, referred to as the MTIC gap, amounted to between €12.5 and €32.5 billion over the 14-year period from 2010 to 2023.

In tackling VAT fraud, another aspect worth mentioning is that studies of the European Union institutions aim to identify which goods are considered more at risk of MTIC VAT fraud. The European Commission's VAT compliance gap due to Missing Trader Intra-Community (MTIC) fraud is the most important source on this topic because it provides the most recent, data-driven, and comprehensive analysis of intra-EU trade flows. It combines the latest trade data with rigorous machine learning to identify which goods are vulnerable to MTIC fraud. The results are displayed below:



In summary, the analysis showed that the predominant portion of the VAT gap due to MTIC fraud (35%) arose from fraudulent activities involving articles in stone and base metals. Machinery and equipment account for roughly 15% of the overall loss, while chemical products, plastics, and rubber account for about 14%. Vehicles also played a notable role, accounting for around 11%.

b. Real case study: operational procedures of the Italian financial police ('Guardia di Finanza')

Detecting and investigating MTIC fraud requires a coordinated, multidisciplinary approach that combines financial intelligence, forensic accounting, digital analysis, and cross-border cooperation.

This section presents a real case conducted by Italy's financial police, the Guardia di Finanza, and provides a practical example of the methods and procedures used during the investigative process. From an operational perspective, the first step that police and tax administration officers should take to dismantle the criminal network and recover the lost tax revenues is to focus on the identification of "red flags" that practical experience suggests are recurrent when VAT fraud is under review: unusual trading patterns (e.g., high-volume transactions involving newcos) or frequent changes in company ownership or management, non-compliance with VAT filing or significant discrepancies in tax returns.

The investigation was initiated following a proactive intelligence gathering by the Guardia di Finanza, based on risk indicators and data analytics. During the preliminary

assessment, the Guardia di Finanza's police officers in charge of the investigation observed that a company located in southern Italy matched all the features that can usually be noticed when approaching a missing trader company. Indeed, despite its recent incorporation, the volume of commercial dealings was quite impressive; however, the VAT returns were filed, but no payments were made. As a result, notwithstanding the company's apparent legitimacy, its commercial operations lacked economic substance. Another element that raised concerns among the police officers was that the companies in the commercial chain, apart from the broker, had no warehouses or storage facilities to hold the goods supposedly traded.

Once the EPPO – the independent body of the European Union responsible for prosecuting crimes against the EU's financial interests – receives the crime report filed by the national law enforcement agency, the second stage of the investigation begins. The EPPO assesses the evidence collected so far and selects the investigative tools to further the investigation.

As far as the Guardia di Finanza's case at issue is concerned, the competent EPPO submitted cross-border investigation requests (according to art. 31 of EPPO Regulation) to obtain in the Member States of the EU the banking statements of all the companies involved in the (allegedly) fraudulent commercial chain, thereby ensuring a consistent investigative approach. Indeed, when analysing the requested banking statements, the police identified financial behaviour inconsistent with normal commercial activity. The absence of operating expenses (e.g., employees' salaries and wages, office or warehouse rents, legal fees, etc.), rapid funds turnover (within the same day) between legal entities, and frequent cash withdrawals suggested that fraudulent operations were being carried out.

As a result, the case reached the evidential threshold envisaged by the Italian Criminal Procedure Code for wire-tapping the suspects. This surveillance technique played a crucial role in uncovering the structure of the MTIC fraud network; indeed, the wire taps provided direct evidence of coordination among the companies involved (conduits, missing traders, buffers, and brokers), as well as the specific roles and responsibilities of the suspects within the criminal organisation. In addition, the European Delegated Prosecutor organised a joint action day, during which searches and seizures of books and papers were conducted simultaneously across all the Member States involved in the case.

The investigation revealed a sophisticated MTIC fraud involving approximately €500 million in false invoices, resulting in an estimated €100 million in VAT losses. Based on the

evidence collected, thirteen suspects were arrested, and the authorities seized the assets identified as proceeds of the fraudulent operations.

The case presented demonstrated that effective cooperation between Member States is crucial to successfully investigate the MTIC fraud network, highlighting the importance of cross-border investigations in tackling large-scale VAT frauds.

c. Strategic coordination in MTIC Fraud prevention within the EU: EMPACT and digital tools for an integrated approach

EMPACT stands for 'European Multidisciplinary Platform Against Criminal Threats' and is the main framework for combating serious and organised crime through joint operations and intelligence sharing. In 2010, the EU launched the EU Policy Cycle for organised and serious crime, a four-year cycle developed to address the most threatening and harmful crimes.

Since 2022, the EU Council has decided to make the EU Policy Cycle a permanent mechanism for joint crime fighting and has adopted a new set of priorities for the current cycle (2022-2025). At the same time, the EU Council changed the name to EMPACT.

EMPACT follows a 4-year cycle and consists of four steps:

- policy development: the EU-SOCTA (European Union Serious and Organised Crime Threat Assessment), prepared by Europol, identifies a set of key threats based on in-depth analysis of the major crime threats facing the European Union
- policy settings: the European Council sets and identifies a limited number of priorities
- development, implementation, and monitoring of operational action plans (OAPs)
- independent evaluation and assessment: at the end of each EMPACT cycle, an independent evaluation will be conducted to assess EMPACT's implementation and outcomes.

The key features of EMPACT are:

- the intelligence-led approach based on a future-oriented and targeted approach to crime control, focusing upon the identification, analysis and management of persisting and developing problems or risks of crime
- the integrated character, best using and aligning the complementary contributions of all multidisciplinary and multi-agency actors from Member States, EU institutions and agencies, as well as relevant third countries and organisations
- the multi-disciplinary, integrated, and integral approach to target the multiple levers of serious and organised crime, i.e. addressing all levels by which a phenomenon can be influenced

These represent the main crime areas the EU will focus on for the current cycle (2022-2025):

- high-risk criminal networks
- cyber-attacks
- trafficking in human beings
- child sexual exploitation
- migrant smuggling
- drug trafficking
- environmental crimes
- organised property crime
- firearms trafficking
- fraud, economic and financial crime

Each area can be divided into sub-priorities and, as far as the EU crime priority on "fraud, economic and financial crimes" is concerned, it consists of five sub-priorities, including MTIC (VAT) Fraud.

This sub-priority aims to "*disrupt the capacity of criminal networks and individual criminal entrepreneurs involved in Missing Trader Intra Community (MTIC) fraud*". Italy plays a pivotal role in addressing MTIC (VAT) Fraud, as the Guardia di Finanza, Italy's financial police, drives this sub-priority by organising, coordinating, and reporting on all EU-wide actions in this crime area. Without a driver country, EMPACT would be too broad and uncoordinated. During last year (2024, EMPACT 2024 Results Factsheets published by Europol), significant results were achieved in tackling MTIC fraud, including 123 arrests, seizures totalling € 583.448.593, and 50 investigations initiated.

Cross-border trade and digitalisation have made the VAT fraud prevention and countering system more challenging for national tax authorities. In response, the EU has developed a network of administrative cooperation mechanisms to detect irregularities before they result in actual fraud. The main pillars of this cutting-edge fraud prevention network are the Vat Information Exchange System (VIES), Eurofisc, the Transaction Network Analysis (TNA) and the Central Electronic System of Payment Information (CESOP).

To have a comprehensive understanding of how these digital instruments work, it is useful to start with the VIES, probably the most well-known tool. The VAT Information Exchange System allows taxpayers to validate a VAT number and obtain basic information about a business entity in another Member State. Access to the website is free and, under Italian law, is granted to everyone in accordance with the provisions of Article 35-*quater* of Presidential Decree 633/1972. Indeed, by using the aforementioned tool, an Italian taxpayer can obtain full disclosure of a customer's VAT number status in another Member State and possibly identify a missing trader abroad. In other words, VIES helps tax authorities and taxpayers prevent fraud at the very first stage. Another important characteristic of VIES is that it acts as a digital hub for the recapitulative statements that taxpayers must submit to tax authorities when performing intra-Community acquisitions or sales of goods and services. The information provided is used both for statistical purposes and for implementing the TNA.

Eurofisc operates under Council Regulation (EU) No. 904/2010, enabling EU countries to share targeted intelligence and early warning signals about suspicious traders. Eurofisc is a network of liaison officials (ELOs) from Member States, designed to exchange information swiftly and coordinate actions against VAT fraud. The system operates through "working fields", each focused on a specific aspect of the VAT fraud-tackling strategy. The most relevant is Working Field 1, which targets Missing Trader Intra-Community Fraud and fraud committed through abuse of customs procedures. In recent years, Working Field 5, which focuses on e-commerce fraud, has gained prominence.

What makes Eurofisc so remarkable for the anti-fraud strategy is its operational and active nature; European Liaison Officials from different Member States cooperate and share targets characterised by a high-risk profile and correctly qualified as missing trader, buffer, broker, etc.

As the volume of intra-Community transactions and the complexity of data increased, the EU needed to develop a technological tool to process this vast amount of information. This

led to Working Field 6, which aimed to implement data analysis software. Working Field 6 was closed in 2021 when Transaction Network Analysis (TNA) became operational. TNA is an analytical software that allows ELOs to detect suspicious supply chain activities among European traders at an early stage. It collects information from the VIES and operates on graph theory and network science. It is used to examine the interrelations between companies engaged in commercial activities within the EU. The TNA platform utilises a combination of algorithmic anomaly detection, behavioural profiling, and risk scoring mechanisms to classify entities based on their likelihood of engaging in fraudulent activity. The results of this analysis are then disseminated via Eurofisc, enabling real-time alerts and administrative actions (e.g., deactivation of VAT numbers, withholding of VAT refunds, targeted audits).

The e-commerce sector has created new challenges for VAT collection, particularly due to the rise of small online sellers and third-country platforms operating from abroad. To fill the gap, the EU introduced the Central Electronic System of Payment Information (CESOP), which entered into force in January 2024. CESOP, introduced in the EU legal framework according to Directive (EU) 2020/284 and Regulation (EU) 2020/283, requires Payment Service Providers (PSPs) – such as banks and online payment platforms – to report to their tax authorities certain data concerning cross-border payments that will be transmitted to a central EU database. CESOP added a new layer of information to the fight against VAT fraud and VAT evasion, using payment data as a powerful tool; for instance, if a third-country e-commerce platform receives payments from EU consumers and fails to register in an EU country for VAT purposes, this can identify a huge red flag of VAT evasion.

Examining the four tools (VIES, Eurofisc, TNA, and CESOP) and their ongoing development, it is worth noting that, over time, the EU counter fraud strategy has shifted from a national-focused approach to an integrated, international model of cooperation based on data and technological tools.

2.1.2. The Common Agricultural Policy scenario in Italy

The Common Agricultural Policy provides Italy with an impressive amount of resources to support the entire agricultural sector, serving as an effective tool for companies, individuals, and public authorities operating in this sector.

The Italian economic set-up is quite sophisticated and can be described as one of the most agriculturally-centred in Europe, due to high production levels, extensive land area, and the large number of people, companies, and authorities involved.

This means that CAP resources play a key role in our Country's economy and all the fraud episodes related to them can represent a serious threat to the internal balance and production mechanisms, with unpredictable consequences.

One of the most well-known features of the CAP is its structure, which is mainly characterised by two Funds (FEAGA and FEASR), each with its own procedures and normative framework for petitioner selection.

The resources related to FEAGA, which are entirely provided by the EU, according to the European and Italian legal frameworks, are distributed according to a specific request presented by farmers, companies or individuals, who, according to Italian rules, have to declare fields on which they're working, even demonstrating the reason why those spaces are available.

FEASR resources follow a different pattern, very often managed by local Administrations, and are usually placed after a long and structured procedure, similar to those of Cohesion Politics. As a matter of fact, those funds are given with the expectation that the recipient will realise a specific activity, project, or, sometimes, structure. In some cases, funds are needed to renew particular tools or machinery used in production processes, for example, to meet new environmental requirements.

The main difference between those patterns, one related to FEAGA and the other used for FEASR, lies in the fact that FEAGA resources are deployed based on the identification of the petitioner as "*active agricultural entrepreneur*", without requiring a specific activity to be performed, except for taking care of the lands owned (farming, breeding, or grazing).

The most important aspect of the domestic legal framework – which derives from the obligations imposed by the EU – concerns the requirement that the standard form of petition for FEAGA's funds (the DUP – *Domanda Unica di Pagamento*), include all evidence proving the applicant's lawful possession of the land declared.

In a few words, the form must be completed with information about the grounds and the activities to be performed on them, in accordance with EU regulations. The Italian Agency responsible for managing PAC resources, AGEA, has mandated the submission of

supplementary documents demonstrating the *connection* between the applicant (individual or company) and the areas where agricultural activities will be conducted.

In reality, the petitioner has to prove the lawful disposition of the ground that is going to be used for agricultural purposes. The provision is studied to avoid or reduce the risk associated with the indication of lands that are not owned, unavailable, or even unsuitable for the activities declared.

a. Fraud schemes

In the last five years, the Guardia di Finanza has investigated expenditure processes related to FEAGA resources, highlighting the system's weaknesses, especially those directly related to the indication of the legitimate ruling (and possession) of the grounds specified in the DUPs. It is important to underline that the number of lands, their extent, and the activities declared are elements that directly affect the calculation of the amount accorded by AGEA.

Exploiting the advantages of having a specific attitude towards investigating all crimes related to economic and financial areas, the analysis process defined the scenario, highlighting the most common fraud trends observed, selecting the most vulnerable steps of the delivery process and suggesting some tips and structural solutions to avoid, or at least to reduce, the risks related to the weak points discovered.

First, it should be said that Italy has a unique framework of organised and "*common"* crime, both of which, as evidence suggests, are interested in obtaining EU resources, because, especially for those coming from FEAGA, there's no required activity to be performed with them.

In more detail, the most common weak points have been identified in the self-declarations of the grounds owned by the percipients and in the related documentation aimed at demonstrating a real existing *link* between the lands and the petitioners.

This specific kind of behaviour has manifested in different patterns, with slightly modified fraud schemes varying from one region to another, depending on the most common crime organisations operating there.

For example, in Southern Italy, where organised crime is settled, most cases involve a threatening dynamic used to force real owners to make land available to certain companies, by

having them sign fake rental contracts and insert them into the DUP, artificially creating the needed link described before. Those cases have been discovered during specific investigations, or, sometimes, because the petitioners were linked with organised crime in person, through figureheads or dummy companies.

In other events, the fraud scheme was basically the same, performed by the use of fake rental contracts, but the main differences have been found in the position of the real owner: sometimes aware, so a partner in crime, sometimes unaware of what happened, or, in some cases, already dead. In some instances, the lands indicated were unavailable because they were included in areas classified as "country property," such as rivers, beaches, and some mountain areas within local or national parks. In some cases, those areas have been indicated as exploited for grazing activities, not suitable for the kind of animals declared: just think of all the logistical troubles that a company would have to face in its effort to make grazing possible for cows on top of a mountain like the Gran Sasso d'Italia (an elevation of more than 2.900 meters).

b. Real case scenario

In 2024, the Nucleo di Polizia Economico–Finanziaria in Pescara, in central Italy, concluded a complex investigation into the described dynamics.

In that specific operation, an important role was played by intelligence activities, which, even before the real investigations "on the ground" began, were able to define some of the emerging fraud trends, or risky behaviour in terms of fraud events, most commonly observed in the area, which is to be found in the central Italy, involving mainly the area corresponding to the Abruzzo region.

The analysis showed that several lands were formally rented by companies and individuals whose headquarters were far from the lands they wanted to use. Due to the fact that the most indicated activity reported by the locators was grazing, and considering that moving large amounts of animals for hundreds of kilometres would be a very demanding task and probably not economically viable, a list of companies was selected and reported, suggesting further activities aimed at investigating whether the rental contracts indicated in the DUPs should be considered fake. The hypothesis was to verify whether those documents were

provided solely to obtain resources from the FEAGA, without performing any of the activities declared.

After receiving the information, backed up by a summary of the risk indicators used, one of the operational units began an investigation, exploiting all the capabilities that the status of law enforcement Agency provides to Guardia di Finanza.

Following the evidence presented in all documents related to achieving FEAGA resources, investigators from the Nucleo di Polizia Economico – Finanziaria in Pescara examined the complex situation involving Abruzzo, Puglia and several areas of the Country.

Pushing forward, some elements directed the investigation towards small groups of individuals linked to organised crime and a dangerous mafia-derived group (named Sacra Corona Unita, based in Puglia, with an area of influence near Foggia). These were the last users of the resources obtained. Employing advanced techniques, such as GPS tracking, mobile phone tracking, and wiretapping, investigators found that a sophisticated network of individuals, companies, and crime figures operated to obtain FEAGA resources. The framework revealed by the one-year-long investigation made clear that the repeated use of fake rental contracts made land available and suitable for a selected number of companies ruled by figureheads, as indicated by the DUP's lands used for grazing activities.

Most of the perpetrators never used the lands declared, causing serious damage to the local economy due to their activities aimed at stealing funds from the available budget. In several instances, rental contracts were also signed after threats to the land's owners, a typical operating pattern of organised crime.

2.1.3. Combating MTIC Fraud: The Italian Criminal Law Framework

It is well established that value added tax operates through a specific mechanism whereby the right to deduct input VAT – arising for economic operators following B2B supplies – may be improperly exploited to obtain undue financial advantages within the framework of fraud schemes organised across more than one Member State. In particular, it is acknowledged that intra-EU exports are not treated as taxable transactions. The typical fraud scheme, therefore, involves at least three undertakings: a first company, A, that supplies goods

to a second shell company, B, located in another EU Member State, which purchases them without paying VAT. Company B (the so-called *missing trader*) subsequently resells the goods to a third company, C, within the same State, collects the tax, and then disappears. Company C then seeks reimbursement of the VAT paid on purchases from company B, thus generating a double loss for the EU budget. The term 'carousel fraud' derives from the fact that, in many cases, company C resells the goods back to company A through a non-taxable intra-EU transaction, thus allowing the cycle to restart.

The scheme described in section 2.1.1. provides a paradigmatic illustration of the operational activity carried out by the Guardia di Finanza in such cases. Taken together, the case study mentioned and the agricultural study discussed below offer an ideal analytical vantage point for assessing how the Italian legislator has shaped the overall enforcement architecture across both the criminal and the administrative dimensions.

From a strictly criminal law perspective, the core issue in MTIC fraud is determining which tax-related offences may be triggered to counter the operations described above.

As regards the conduct of the party issuing the first invoice, the offence laid down in Article 8 of Legislative Decree No. 74/2000 (renumbered, as of 1 January 2026, as Article 79 of Legislative Decree No. 173/2024) is clearly applicable (D'Arcangelo 2017, 261 ff.; Soana 2023, 293 ff. Lanzi, Aldovrandi 2020, 497). This provision criminalises any person who, with the intent of enabling third parties to evade income tax or value added tax, issues or releases invoices or other documents for non-existent transactions. For the purposes of this offence, the expression "invoices or other documents for non-existent transactions" – by explicit legal definition – refers to invoices and any other documents with equivalent probative relevance under tax law (pursuant to Article 21 of d.P.R. No. 633/1972), issued in respect of transactions that have not actually been carried out, in whole or in part, or that indicate consideration or value added tax in excess of the actual amount, or that attribute the transaction to persons other than the real parties involved. Moreover, although part of the scholarly literature considers only substantive falsehoods to fall within the scope of the offence (Lanzi, Aldovrandi 2020, 215; Aldovrandi 2019, 281 ff.), the prevailing view maintains that material falsifications are also criminally relevant. With regard to non-existence, the operation of the provision is undisputed in cases of objective non-existence of the transaction – that is, situations in which the goods have never been genuinely supplied or purchased.

Concerning cases of mere interposition – which also encompass a substantial portion of carousel-fraud schemes – the relevant figure is that of 'subjective non-existence' (i.e., fictitious interposition of parties) (Falsitta, Fagioli 2017, 37 ff.; Soana 2023, 126 ff.). In these circumstances, part of the scholarly literature distinguishes between situations in which the interposition is directly aimed at securing an undue tax advantage through a fraudulent agreement among the various parties involved, and those in which the interposition consists in the mere participation of an entity that has no economic rationale for intervening in the transaction other than obtaining tax benefits. In the latter scenario, the scheme should fall within the paradigm of abusive tax planning (pursuant to Article 10-*bis* of Law No. 212/2000), which, as an expression of abuse of law, does not give rise to criminal liability (Bellacosa, 2016, 300 ff.; Lanzi, Aldovrandi 2020, 498 f.). It must nevertheless be emphasised that, in MTIC fraud, the interposition of a missing-trader company is coupled with a direct and manifest violation of tax law. In such circumstances, no doubt arises as to the tax evasion purpose of the conduct.

Likewise, regarding the invoice issued by the missing trader, the offence under the aforementioned Article 8 may be established, since the conduct enables the third company to deduct VAT that has only apparently been paid. Conversely, a recipient who uses such a document in its tax return is liable for the offence set out in Article 2 of Legislative Decree No. 74/2000 (renumbered, as of 1 January, as Article 74 of Legislative Decree No. 173/2024), which criminalises any person who, with the intent of evading income tax or value added tax by relying on invoices or other documents relating to non-existent transactions, includes fictitious deductible items in one of the relevant tax returns (Ruta 2017, 193 ff.; Lanzi, Aldovrandi 2020, 498; Soana 2023, 378 ff.). It is worth emphasising that, in such cases, cumulative liability for the latter offence and the aggravated fraud against the State under Article 640-*bis* of the Criminal Code is excluded, as Article 2 is deemed to absorb the whole wrongful content of the conduct (Cass. pen., Sez. Un., 28 October 2010, n. 1235).

It must also be noted that the applicability of Article 8 to intermediaries or to the missing-trader entity does not depend on the actual use of the invoices by the recipients; accordingly, the offence is committed at the time when the false document is transferred, dispatched, or made available, irrespective of whether the user subsequently files a tax return. This qualification is crucial in the context of carousel fraud, where the issuer does not coincide,

by definition, with the party recovering the undue deduction and is instead structurally designed to disappear after a brief operational phase.

Lastly, if the missing trader disappears without filing the required tax returns, the offence set out in Article 5 of Legislative Decree No. 74/2000 (renumbered, as of 1 January, as Article 77 of Legislative Decree No. 173/2024) is also established. This applies since – provided the same specific intent referred to above is present – the provision criminalises any person who fails to file tax returns, in the present context those relating to VAT (Lanzi, Aldovrandi 2020, 418 ff.; Soana 2023, 261 ff.). Conversely, where the tax returns are filed, but the tax remains unpaid, the offence of failure to pay VAT – recently amended by Legislative Decree No. 87/2024 – applies (Musco, Ardito 2021, 340 ff.; Ambrosetti, 2022, 499 ff.; Martini 2010, 591 ff.; Perini 2008, 162 ff.). In particular, this provision now applies where the unpaid VAT exceeds seventy-five thousand euros, and the taxpayer fails to enter into, by 31 December of the year following the filing of the annual tax return, the instalment plan provided for by the relevant special legislation (Article 3-*bis* of Legislative Decree No. 462/1997) (Ingrassia 2024, 1570; Ardizzone 2025, 13 ff.).

Against this highly fragmented regulatory background, corporate liability under Legislative Decree No. 231/2001 becomes relevant following the implementation of the PIF Directive. The transposition of the Directive took place in two stages. The first stage, via Decree-Law No. 124/2019, involved inserting Article 25-*quinquiesdecies* into the above-mentioned Legislative Decree, thereby extending corporate liability to the most serious tax crimes, including the offences established in Articles 2 and 8 of Legislative Decree No. 74/2000. As a result, since 2019, the "core" offences for combating carousel fraud have been part of the catalogue of predicate crimes that trigger corporate liability. Furthermore, the same decree increased the penalties for the two offences, thus strengthening the overall punitive response (Ingrassia 2020, 307 ff.).

Subsequently, Legislative Decree No. 75/2020 – the formal instrument of transposition of the EU Directive – added the offence of failure to file tax returns under Article 5 of Legislative Decree No. 74/2000 in order to further enforcement, particularly vis-à-vis missing-trader companies that disappear without filing the relevant tax returns. This inclusion was expressly intended to strike more severely at carousel-fraud schemes. Following the reform introduced by Legislative Decree No. 156/2022, the provision applies to legal persons only where the offence is committed with the aim of evading value added tax within cross-border

fraudulent systems connected to the territory of at least one other EU Member State, resulting, or likely to result, in overall damage amounting to at least ten million euros, mirroring the wording of the PIF Directive itself (Bellacosa 2020, 611 ff.). Conversely, the standalone offence of failure to pay VAT does not currently form part of the catalogue of predicate crimes. Consequently, where the missing-trader company files the relevant tax returns but fails to pay the tax due, it will only be liable for the offence of issuing invoices for non-existent transactions, provided that one of its senior managers or subordinates engaged in such conduct with the intent of enabling the third company in the fraudulent scheme to evade VAT, without prejudice to the liability of the natural person.

This analysis confirms that the Italian regulatory and enforcement framework appears to be substantially aligned with the European *acquis*. The various stages of the fraudulent chain are comprehensively addressed by distinct criminal provisions tailored to the specific factual conduct of each operator involved, whether a natural person or a legal entity. Consequently, no meaningful areas of impunity persist within the domestic system.

2.1.4. The Domestic Sanctions Regime for CAP Fraud

Operation "*Transumanza*", analysed in the above-mentioned case study (section 2.1.2), provides an ideal vantage point for observing the concrete operation of the criminal provisions safeguarding EU agricultural funds. The fraudulent pattern that emerged is centred on the systematic indication, within the single payment applications, of non-existent or fictitious entitlements to use agricultural land formally "made available" to companies linked to criminal associations, sometimes through simulated lease agreements or leases extorted from the actual landowners, and at other times through the artificial valorisation of State-owned or otherwise unavailable areas. A scheme of this kind aptly illustrates the core problem of the regulatory framework: the declaratory phase of the procedure governing access to CAP payments, and, in particular, the role of the false representation of the relationship between the beneficiary and the land as a tool for the unlawful appropriation of EAGF and EAFRD resources (Carmignani, Papini, 2022, 203 ff.).

It is at this stage of the causal sequence – namely, the submission of the aid application to the Paying Agency, accompanied by data and documents attesting to the (non-existent)

availability of the land and the alleged performance of agricultural activities on it – that the three main offences currently applicable come into play: Article 2 of Law No. 898 of 23 December 1986, the aggravated fraud for obtaining public funds under Article 640-*bis* of the Criminal Code, and the offence of unlawful receipt of public funds under Article 316-*ter* of the Criminal Code (Mazzanti, 2020, 106 ff.).

As previously described (D2.3, par. 9.1.1), subsequent to the transposition of the PIF Directive, it is well established that the nerve centre of criminal law safeguards against CAP fraud is to be found in Article 640-*bis* of the Criminal Code, which sanctions with imprisonment from two to seven years fraud involving grants, subsidies, financing, subsidised loans or other similar public disbursements, however designated, granted, or disbursed by the State, other public bodies, or the European Union (Pelissero 1991, 923 ff.; Gullo 2000, 528 ff.; Mezzetti 2010, 316 f.; Bisori 2021, 7284 ff.). The material scope therefore encompasses payments financed through the EAGF and the EAFRD, so that whenever the fraudulent conduct is carried out through artifice or deception capable of misleading the Paying Agency – as in situations where the documentary construction surrounding simulated lease agreements is such as to make the alleged title to the declared land surfaces appear credible – the aggravated fraud for obtaining public funds constitutes the ordinary offence of reference. At the same time, Articles 316-*ter* of the Criminal Code and Article 2 of Law No. 898/1986 operate in a subsidiary capacity.

The reform implementing the PIF Directive has markedly increased the punitive response: on the one hand, by extending to the offence the general applicability of mandatory confiscation of the proceeds, including by equivalent, pursuant to Article 322-*ter* of the Criminal Code; on the other hand, by including Article 640-*bis* in the catalogue of offences linked to the so-called "extended confiscation" under Article 240-*bis* of the Criminal Code, with the consequence that, once disproportion between the convicted person's assets and their lawful income is established, it is now possible to seize the entirety of their patrimonial portfolio beyond the strict limit corresponding to the profit generated by the individual fraudulent episode (Picciotti 2020).

On a partially overlapping plane lies Article 316-*ter* of the Criminal Code, introduced to implement the PIF Convention and now reinterpreted in light of the new EU framework. The provision – which substantially mirrors the conduct described in Article 2 of Law No. 898/1986 – criminalises the unlawful receipt of public funds to the detriment of the State or

another public body, imposing a custodial sentence corresponding to that provided for under the aforementioned Article 2. It sanctions both the submission of false data or documents and, in addition, the "omission of information that ought to be disclosed", a form of conduct not contemplated by the special offence governing agricultural subsidies (Pelissero 2001, 991 ff.; Romano 2002, 269 ff.; Id. 2013, 82 ff.; Seminara 2017, 1026 ff.; Amarelli 2018, 79 ff.).

Here too, the conduct is downgraded to an administrative offence below a quantitative threshold (broadly corresponding to that provided for under Article 2 of Law No. 898/1986). Once that threshold is exceeded, the application of the criminal provision entails mandatory confiscation of the proceeds – including value-based confiscation – pursuant to Article 322-*ter* of the Criminal Code, as well as extended confiscation under Article 240-*bis* of the Criminal Code, in addition to the accessory penalty of disqualification from contracting with public authorities.

In this setting too, the relationship with Article 640-*bis* of the Criminal Code is governed by a principle of subsidiarity: where the conduct of the agent actually succeeds in inducing the disbursement authority into error, the scenario falls within aggravated fraud for obtaining public funds; only where the typical structure of fraud is absent (although the benefit has been obtained through the submission of untruthful declarations or through silence in respect of legally relevant information) does Article 316-*ter* of the Criminal Code retain autonomous applicability (Manacorda 2001, 424; Romano 2002, 271 f.; Basile 2020, 184; Cass., Sez. Un., 19 April 2007, n. 16568).

Against this backdrop lies the earliest and most closely tailored provision to the phenomenon of CAP fraud, namely Article 2 of Law No. 898/1986, rightly described as the "archetype of Community frauds *tout court*" (Mazzanti 2020, 111; Mezzetti 2010, 319 f.). The provision imposes a sentence imprisonment from six months to three years on any person who – unless the conduct constitutes the more serious offence under Article 640-*bis* of the Criminal Code – by submitting false data or information, unlawfully obtains for themselves or for others aid, premiums, indemnities, refunds, contributions or other disbursements financed, in whole or in part, through the EAGF or the EAFRD. Where the unlawfully obtained amount is lower than five thousand euros, the conduct falls exclusively within the administrative offence set out in Article 3 of the same statute. The reform implementing the PIF Directive (Legislative Decree No. 75/2020 and the corrective Legislative Decree No. 156/2022) has affected three qualifying aspects: it reaffirmed the obligation to return the unlawfully received amount; it extended to

this offence the mandatory confiscation of the proceeds – including by equivalent – pursuant to Article 322-*ter* of the Criminal Code; and it finally brought the offence within the scope of "extended confiscation" under Article 240-*bis* of the Criminal Code.

In resolving the apparent conflict between the relevant criminal provisions, although part of the case law applies Article 316-*ter* of the Criminal Code also in agricultural-fund fraud cases (Cass., Sez.VI, 9 june 2016, n. 32730; Cass., Sez.VI, 3 march 2022, n. 15620), the correct approach is to consider that only Article 2 of Law No. 898 should apply – as the special provision in view of its material scope (Ardizzone 2024, 24 ff.) – or, alternatively, Article 640-*bis* of the Criminal Code where the conduct succeeds in inducing the Paying Agency into error, given the subsidiarity relationship between the latter offence and the other two (Gullo 2000, 532; Picotti 2006, 628 ff.; *contra*, Mezzetti 2010, 323 f.).

On the administrative side, Article 3 of Law No. 898/1986 provides a parallel – and structurally cumulative – system of protection alongside the criminal offences mentioned above. The provision imposes a financial penalty equal to the amount unlawfully obtained in the case of aid financed through the EAGF, or calculated as a percentage of the amount disbursed – up to a ceiling of 150,000 euros – in the case of EAFRD contributions, for the same conduct described in Article 2, while in all cases requiring repayment of the undue benefit and, under its fifth paragraph, establishing a prohibition on receiving further benefits from the same authority until the conclusion of the procedure. The clause stating that the administrative sanction applies "independently of the criminal sanction" means that the administrative offence operates even when the conduct is legally classified by the criminal court under Article 316-*ter* or Article 640-*bis* of the Criminal Code, thereby creating a dual-track punitive system which, as has been emphasised, raises serious doubts of compatibility both with the principle of proportionality of the overall sanctioning response and with the *ne bis in idem* principle, in its Convention-based formulation and under the perspective of the Charter of Fundamental Rights of the European Union (Tripodi 2022, 66 and 105 f.).

Finally, as regards collective entities, the transposition of the PIF Directive has marked a significant development: Article 2 of Law No. 898/1986 has been included in the catalogue of predicate offences giving rise to corporate criminal liability under Legislative Decree No. 231/2001. This means that fraud against EU agricultural funds – such as those uncovered in *Operazione "Transumanza"* – may now trigger the liability of legal persons, thereby encouraging them to adopt self-regulatory and preventive organisational safeguards. The

effectiveness of this mechanism, however, is currently attenuated by the persistence of the administrative offence under Article 3 of Law No. 898/1986, which continues to apply – with its accompanying pecuniary sanction and prohibition on accessing further benefits – also to collective entities. The result is a superimposition of punitive tracks on the corporate side, which risks diminishing the "reward" associated with implementing efficient and compliant organisational structures (Ardizzone 2024, 33 ff.).

What emerges from investigative practice in the field of CAP fraud – as the case study clearly demonstrates – is the need for a comprehensive reconsideration of the sanctioning architecture, capable of reconciling, on the one hand, the objective of ensuring effective criminal law protection of the European Union's financial interests and, on the other, full respect for the principles of proportionality and *ne bis in idem*. In this respect, the European-driven criminalisation objectives can be deemed fulfilled: the legal system provides for a complete set of offences capable of covering the typical factual articulations of CAP fraud, both as regards natural persons and, following the transposition of the PIF Directive, legal persons. Residual needs nonetheless emerge in terms of simplification and coordination, in order to ensure greater clarity in identifying the applicable offence and to avoid undue overlaps between the criminal and administrative branches of enforcement, which risk giving rise to tensions with the *ne bis in idem* principle under Article 50 of the Charter of Fundamental Rights of the European Union.

2.2. The analysis of key legal tools emerged from the dialogue with the competent authorities

The Italian chapter closes with a section dedicated to the analysis of some legal tools, processes and structures that emerged as relevant or complementary in the first part.

The sub-paragraphs refer to different phases of the abstract process of combating fraud against the EU's financial interests, starting with reporting suspicious operations (by other institutions and/or citizens) and proceeding to the detection of crimes (and their remedies), passing through controls and institutional collaboration.

For example, while the real case scenarios presented previously by Guardia di Finanz*a* highlighted the role of investigations carried out by the competent authorities *ex officio*, in

many cases, the role of reporting by other administrations and individuals is essential to initiating investigative activities.

In fact, it must be taken into consideration that "prevention" also passes through the definition of whether" and "what" should be reported to the competent authorities, and this is more true today with the RRF (see art. 22, Regulation (EU) 241/2021).

2.2.1. National declinations and operability of the notions "suspected fraud", "suspicious operation". The role of public institutions in reporting cases

As reported in the last BETKONEXT working paper (D2.3, p. 26), irregularities must be reported to the Commission in accordance with Annex XII of Regulation 2021/1060. Irregularities of the first kind are those that have been the subject of a first written assessment by a competent authority, either administrative or judicial, which has concluded based on specific facts that an irregularity has been committed, regardless of the possibility that this conclusion may subsequently have to be revised or withdrawn as a result of developments in the course of the administrative or judicial procedure. Irregularities of the second type are those that lead to the initiation of administrative or judicial proceedings at the national level to establish the presence of fraud or other criminal offences.

In Italy, the Inter-ministerial Circular of 2007 and the related COLAF explanatory notes have led to a distinction in the first administrative or judicial report (PACA, in Italian '*Primo verbale amministrativo o giudiziario*'), from which derives an obligation to communicate through the IMS an irregularity or suspected fraud, between two levels:

1. The administrative level, found in the first act, was created at the end of the evaluation by the decision-making bodies, based on the data and information from the initial challenge report, which was also drafted by the so-called "External Control bodies", such as the police forces;
2. The judiciary level – where it coincides in the ordinary proceeding with the request for prosecution or alternative proceedings, pursuant to Article 405 of the Criminal Procedural Code, in proceedings before a

monocratic Court (in which the public prosecutor proceeds to summon to the court), with the issuance of a summons.

Even though the previous ones can be interpreted as legal definitions, especially at the EU level, where Regulation 2021/1060 is at stake, they do not say anything specific on the "content" of the "suspected fraud", considered as elements of alert in a preventive phase: which are those symptomatic elements, from which duties/obligations of reporting to the competent authorities derives?

It is clear from the previous analysis of real cases that the concrete scenarios are so numerous and diverse that a legal definition of irregularity that could be considered "suspected fraud" would be almost impossible to formulate.

However, in Italy, there are different sectoral disciplines in which the term 'operationalisation' can be observed.

Anti-money laundering

First, the anti-money laundering sector comes into play. Considering the new European package on the issue (see BETKONEXT D2.3, p. 22; cf., for more references BETKONEXT D1.3, p. 35) and the advent of the NRRP (Circular No. 27 of 15 September 2023, the NRRP Inspectorate General of the State General Accounting Office), the fight against money-laundering has become even more delicate than in the past, also because new technologies are enabling the organized crime to take advantage of the financial sector more easily than in the past.

Here, the relevant notion is that of "suspicious transactions". Article 10 of Legislative Decree no. 231 of 21 November 2007 (the so-called Anti-Money Laundering Decree) establishes the duty of Public Administrations to notify the FIU of any suspicious transactions detected in the performance of specific activities.

Article 10 establishes first of all that its obligations concern the offices of the public administrations responsible for carrying out tasks of active administration or control, in the context of procedures aimed at the adoption of authorisation or concession measures, procedures of choice of contractor for the awarding of works, supplies and services in accordance with the provisions of the Public Contracts Code and procedures for the granting

and disbursement of subsidies, contributions, grants, financial aids, as well as allocation of economic advantages of any kind to natural persons and public and private entities.

The public offices engaged in the performance of these functions, in order to allow the performance of financial analyses aimed at uncovering money laundering and terrorist financing phenomena: "shall communicate to the FIU data and information concerning suspicious transactions of which they become aware in the course of their institutional activity" (art. 10, Anti-Money Laundering Decree) and, to this end, in the framework of their continuous staff training programmes, they shall adopt appropriate measures to ensure that their employees recognise the cases deserving to be communicated under the same provision.

The latter also provides that the Financial Security Committee operating at the Ministry of Economy and Finance, also on the basis of the national risk analysis, will identify categories of administrative activities, carried out by the Public Administrations in charge of the above-mentioned procedures, with respect to which the obligations mentioned above do and do not apply.

The FIU, in specific instructions adopted after consultation with the Financial Security Committee, identifies the data and information that the Public Administrations must transmit, the modalities and deadlines for the relevant communication, as well as the indicators to facilitate the detection of suspicious transactions.

Consequently, with a provision of 23 April 2018, the FIU issued the implementing rules of the cited Article 10, establishing, first of all, that the Public Administrations required to communicate to the FIU data and information concerning "suspicious transactions" must do so, regardless of the relevance and amount of the transaction, basing the suspicion on a thorough assessment of the objective and subjective elements acquired in the context of the institutional activity carried out (Report by the Italian Afcos, Measure for prevention and fight against frauds and other crimes at the detriment of the NRRP, 2024, 56).

The prerequisites for identifying suspicious transactions are derived from Article 35 of the same Anti-Money Laundering Decree, which states that public offices must make the report: "when they know, suspect or have reasonable grounds for suspecting that money laundering or terrorist financing operations are being or have been carried out or attempted, or that the funds, regardless of their amount, come from criminal activity". The Thematic Appendix attached to Circular No. 27 of 15 September 2023 from the PNRR General Inspectorate specifies that "in this context, the suspicion that the subject with whom the

Administration has relations is involved in illicit activities or may exploit for illicit purposes the relationship with the Public Administration or the funds deriving from the NRRP is also relevant". The assessment of the objective and subjective elements acquired in the context of the institutional activity carried out, from which to base the eventual communication, may also rely on the anomaly indicators reported in the annex to the same provision of 23 April 2018. The purpose of the latter is to reduce the margins of uncertainty of the subjective assessments associated with the reporting of suspicious transactions and to contribute to the containment of burdens, as well as the correctness and homogeneity of the reports themselves.

As observed in the Italian AFCOS's Report of 2024 (pp. 55-56), the list of such anomaly indicators is not exhaustive, given the continuous evolution of the way transactions are carried out. The impossibility of linking transactions or conduct to one or more of the indicators is not sufficient to exclude that the transaction is suspicious; therefore, further conduct and characteristics of the transaction, which, although not described in the indicators, are equally symptomatic of suspicious profiles, should be assessed with the utmost care. On the other hand, the mere recurrence of transactions or conduct described in one or more anomaly indicators is not in itself sufficient reason for qualifying the transaction as suspicious for the purposes of reporting it to the FIU, but it is in any case necessary to carry out a specific analysis in concrete terms and an overall assessment of the transaction using all the other information available.

The report is also sent to the FIU when public authorities have data and information relating to transactions that have been refused, discontinued, or executed in whole or in part with other recipients with independent reporting obligations.

The reporting of data and information concerning suspicious transactions to the FIU is a separate act from the reporting of criminal offenses, which public officers and persons in charge of a public service are required to make, pursuant to Article 331 of the Code of Criminal Procedure, when, by virtue of their functions or because of their office or service, they "have knowledge of a crime that is prosecutable *ex officio"* and which is based on the identification of specific facts corresponding to a criminal offense. In any case, the public administrations ensure the utmost confidentiality of the identities of the individuals making the disclosure and of the content.

The content of the communication consists of 1) identifying data, containing the information that identifies and qualifies the communication and the Public Administration; 2) information elements, in structured form, on the transactions, subjects, relationships and the

links between them; 3) descriptive elements, in free form, on the operations covered by the communication and the reasons for the suspicion; 4) any attached documents.

Regarding the information elements in "structured form", these must relate to the transactions, relationships, the persons to whom the administrative activity relates, the links between the transactions and relationships, the links between these and the persons, and the links between the persons. The report contains a reference to at least one transaction and to the subject to whom it relates, and may contain a reference to several transactions that appear to be functionally or economically connected; it may also include transactions that are deemed not suspicious if necessary for an understanding of the operations described or of the suspicion expressed.

As part of the free-form descriptive elements, reference should be made to the economic and financial context, illustrating in a comprehensive and detailed manner the grounds for suspicion, i.e. the reasons that led public authorities to suspect the transaction of being linked to money laundering or terrorist financing and to make the report. In particular, the logical process followed by public authorities in assessing the anomalies detected in the transactions covered by the report must be clearly explained.

Public authorities must, by formal provision, designate a "manager" as the subject to whom the assessment and communications are delegated to the FIU. In this regard, the Thematic Appendix attached to the above-mentioned Circular no. 27 of 15 September 2023 of the General Inspectorate PNRR suggests that the Public Administrations should consider appointing, as manager, the same person who performs the function of 'Person in charge of the prevention of corruption and transparency', to improve the integration between anti-money laundering and corruption prevention measures. On this point, the Appendix, recalling the indications provided by the National Anti-Corruption Authority in the National Anti-Corruption Plan approved on 16 November 2022 and valid for the following three years, points out that in any case, adequate synergies between the anti-money laundering and anti-corruption provisions present within each administration must be ensured. With such precautions, administrations can identify the anti-money laundering manager as part of the control function for NRPP purposes.

The operator must subscribe to the Infostat - FIU portal and use it for all interaction with the FIU, ensuring timely communication, maximum confidentiality and prompt reconstructability of the reasons underlying the decisions taken. He receives and analyses

information from public office staff concerning any anomalies intercepted in transactions and conduct referable to the persons with whom they deal, and assesses from time to time the advisability of transmitting a suspicious transaction report to the FIU.

Focus. Anti-money laundering and NRRP

With regard, specifically, to the NRRP, with its Communication of 11 April 2022, the FIU preliminarily remarked the importance of bringing to its attention with the utmost timeliness any suspicious transactions concerning the Plan itself, so as to allow the activation of internal cooperation and international cooperation and also the possible exercise of the power of suspension provided for by Article 6, paragraph 4, letter c) of Legislative Decree no. 231 of 2007. In this regard, with the Communication of 31 May 2022, the FIU, in order to facilitate active cooperation and to enable its structures to promptly detect the contexts in which anomaly profiles are detected both in the phase of access to the resources of the Plan, and with reference to their use, introduced a new 'taxonomy' indicative of the specific phenomenon that the reporting persons must use, called 'PN1 - Anomalies related to the implementation of the PNRR'. With a subsequent Communication of 20 May 2023, the FIU introduced additional codifications to facilitate the traceability of the suspicious transactions reported to each mission of the Plan.

The Communication of 11 April 2022 (as shown here, 59), stresses how a further useful safeguard also for anti-money laundering purposes is to be found in the provision in Article 9, paragraph 4, of Law Decree no. 77/2021 (the 1st NRRP governance decree), which establishes that in the implementation of the NRRP interventions, authorities must ensure the complete traceability of the transactions and the keeping of a specific accounting codification for the use of the resources in accordance with the indications of the Ministry of Finance. All acts and relevant supporting documentation are maintained on computer systems and are available for audit control activities. It is therefore appropriate to guarantee the relevant competent authority, for communication with the UIF, full access to information and documentation concerning the implementation of the projects and the reporting of expenses.

The communication also recalls that Article 22 of Regulation (EU) 2021/241, which establishes the RRF, imposes an obligation to collect certain categories of data to protect the EU's financial interests. It explicitly requires that, for recipients of funds and contractors, the

beneficial owner be identified as defined in the anti-money laundering rules. To this end, it is appropriate for public administrations to consider the concepts and guidelines outlined in the Anti-Money Laundering Decree, utilise public or private databases where accessible, and maintain evidence of the criteria followed to identify beneficial ownership. This clarification is even more relevant given that public administrations are not currently considered entities subject to the anti-money laundering obligations specified in Article 3 of Legislative Decree No. 231 of 2007 and are therefore not entitled to access the National Register of Beneficial Owners under this Article. 21(2) and (4) of and Ministerial Decree no. 55 of 11 March 2022, such access being allowed–among others–to "obliged persons", as support for the obligations prescribed during due diligence. For the identification of the beneficial owner, the public administrations must, of course, refer to the specific Thematic Appendix attached to NRRP Circular No. 27 of 15 September 2023 (as mentioned above).

What has emerged until now regarding suspicious operations in the light on the anti-money laundering strategy for the NRRP (see here), is that among the most frequently detected triggers of active collaboration are: recent establishment of the company or change of registered office, name, sector of activity, governance, in proximity to the request for access to financing; the absence of employees or a website in the face of a significant turnover; the late approval of financial statements; the recent and sudden increase in turnover; opaque shareholding chains preventing the correct identification of the beneficial owner; difficulty in providing supporting documentation or possible forgery thereof; poor handling of reports in the phase prior to the crediting of resources; inconsistent use of funds with respect to the purposes of the measure; links between different applicants that could underlie hypotheses of "double financing" (e.g. same consultants, foreign service providers, outsourcer, beneficial owners, addresses of company headquarters, etc.).

Anti-mafia regulation

Also in the Communication of 11 April 2022 (as reported here, 58), the FIU points out that for the purposes of the use, in relation to the NRRP, of the anomaly indicators for reporting suspicious transactions referred to in the measure of 23 April 2018, particular attention should be paid, in addition to those of a general nature, to the indicators concerning the procurement, public contracts and public financing sectors, emphasizing the importance, for the purposes of

the assessment of economic entities accessing tenders, concessions or other benefits linked to NRRP funds, of timely and effective checks on the so-called anti-mafia documentation. On this point, the Thematic Appendix attached to Circular No. 27 of 15 September 2023, recalled in the previous section, draws attention to the importance of ensuring adequate attention to financial movements and the use of the dedicated current account, taking into account the obligations of the traceability of financial flows laid down by the legislator to combat criminal infiltration in public procurement, in order to promptly detect any suspicions of misuse of funds.

The provisions concerning the so-called "anti-mafia prevention system" focus primarily on the "anti-mafia documentation", and in particular on the "anti-mafia information'" (Legislative Decree no. 159 of 6 September 2011, the so-called Anti-Mafia Code), the application of which is entrusted to the Prefects pursuant to the provisions of the NRRP, are undoubtedly included among the legality safeguards useful to prevent and counteract illicit offences to the detriment of the financial resources referable to the NRRP, especially for the purposes of the evaluation of the economic subjects that access the tenders, the concessions or other benefits connected to the funds of the Plan.

It is now necessary to briefly highlight the elements that the Prefect must assess for the adoption of an antimafia interdiction (for complete references, see the paper by Birritteri and Tatì, 2023, under the BETKOSOL project). One of the key questions here is the interpretation of the notion of "attempts of mafia infiltration", to determine, based on the elements gathered by the Prefect, whether it is possible to establish whether the company can facilitate criminal activities or, at least, be conditioned by them.

This assessment is also regulated by the *Informativa anti mafia* chapter of the Code, which provides the Prefect with the possibility of conducting investigations with respect to subjects who appear to significantly influence the company's choices.

The Prefect can also gather other useful elements to assess the existence of attempted mafia infiltration of the business, hence adopting an interdiction, from judicial decisions or judgements, even if not res judicata, showing that the company is facilitating or being conditioned by criminal activities, as well as from the verification of repeated violations of the financial flow traceability regulations.

The Prefect's powers are quite extensive, especially when he is called upon to assess the existence of criminal infiltration based on elements that are not explicitly regulated by law.

However, over the years, case law has clarified that this assessment shouldn't focus on "judicial evidence"; instead, it should be directed towards "symptomatic" red flags or mere suspicions that indicate a high probability of criminal infiltration into the business, posing a real danger to public order. It is relevant to point out that, to allow the Prefect to do this kind of assessment, the Antimafia Code provides for the possibility of adopting an inter-ministerial regulation aimed at identifying, inter alia, the riskiest sector with respect to Mafia infiltration, thus showing the strong preventive approach of such a system.

Even though this regulation has never been adopted, other solutions have been tested to fulfil this objective, including before the adoption of the Antimafia Code itself. The reference here is to the so-called "Legality agreements or protocols", which were only recently regulated by the legislator in the Antimafia Code to simplify, while at the same time controlling, the economic recovery. These protocols can be considered an alternative method of private participation in the procedures of the antimafia sector, even though they are adopted outside the interdiction procedure. Then, the anticorruption regulation has also created a "whitelist" of Mafia-free operators.

Anti-mafia regulation and NRRP Focus

The Anti-Mafia Code was amended by Articles 47 to 49-*bis* of Decree-Law No. 152 of 6 November 2021 (one of the NRRP Decrees). In a nutshell, the latter measure provided for 1), with Article 47, the amendment of Article 34-*bis* of the Anti-Mafia Code, on the subject of "judicial administration and judicial control of companies"; 2), with Article 48, the integration of the rules on the procedure for the issuance of anti-mafia information, affecting Articles 92 and 93 of the Code, with the provision of forms of cross-examination/right to be heard; c) with Article 49, the insertion into the Code of a new Article 94 bis which provides for the adoption, by the Prefects, of administrative measures of cooperation by the company in respect of which it is ascertained that the attempts of mafia infiltration are traceable to situations of occasional facilitation, by means of a "hybrid" measure, so to speak, i.e. not liberating or prohibitory with respect to the exercise of the business activity, but preparatory to the adoption of the liberating or prohibitory anti-mafia information at the end of the validity period of the measures themselves (Birritteri, Tatì, 2023).

For the functioning of this system, of central importance is the effective use of the Single National Database of Anti-Mafia Documentation (BDNA), the rules of which have been duly updated, with amendments operational as of 17 May 2022, to ensure that, at access to the same database, it is expressly stated whether the request for documentation relates to an intervention implementing the NRRP.

Within the framework of the initiatives aimed at accelerating and streamlining the implementation procedures of the NRRP, Article 14, paragraph 4-bis, of Law Decree No. 13 of 24 February 2023 (one of the latest NRRP governance decrees) has delegated to a specific provision of the Minister of the Interior the identification of measures to strengthen the investigative actions of the aforementioned GIAs established at the Prefectures, utilizing the human, instrumental, and financial resources available under the current legislation. In implementation of the aforementioned legislative provision, the Ministerial Decree of 2 October 2023 was issued, bearing "Measures to strengthen the investigative action of the Anti-Mafia Inter-Force Groups set up at the Prefectures", whose Article 5 also envisages the sharing by the DIA of "any investigative outcomes of potential interest" resulting from the development of reports on suspicious money laundering transactions related to mafia-type associations, subject to compliance with the confidentiality regime established by Legislative Decree no. 231 of 2007 and the investigative secrecy of pursuant to Article 329 of the Code of Criminal Procedure.

The aforementioned GIAs are entrusted with executing access to construction sites ordered by the Prefects, pursuant to Article 93 of the Anti-Mafia Code, which constitutes particularly useful and effective tools for identifying possible infiltrations of organised crime in the executive phases of public works. Briefly, the control takes the form of an on-the-spot check of the natural persons and legal entities present, the equipment, the means employed, and the contractual documentation produced between contracting stations, tenderers, and any third parties involved in subcontracting. The information thus acquired is transmitted to the competent prefectures, which use it to feed the Information System SIRAC, which the Anti-Mafia Investigative Directorate manages. The Prefects, based on what has been found on construction sites, may also intervene in the executive phase of the works by adopting any anti-mafia measures of an interdiction nature, and may even amend the documentation previously issued.

Finally, in the context of preventive and repressive measures against criminal infiltration into the economy, and in particular into public procurement and concessions, two new provisions introduced by Decree Law No 19 of 2 March 2024 (an additional NRRP Decree) are of particular importance.

The first concerns the offence of "fraudulent transfer of assets" referred to in Article 512-bis of the Criminal Code, which, in its original version, provided for a single paragraph stating as follows: "Unless the act constitutes a more serious offence, anyone who fictitiously attributes to others the ownership or availability of money, goods, or other benefits to circumvent the provisions of the law on the prevention of asset laundering or smuggling, or to facilitate the commission of one of the offences referred to in Articles 648, 648-bis, and 648-ter, shall be punished with imprisonment for a term of between two and six years. Paragraph 9 of Article 3 of the aforementioned Decree Law No 19 of 2024 added a second paragraph according to which, "the same penalty referred to in the first paragraph shall apply to anyone who, in order to circumvent the provisions on anti-mafia documentation, fictitiously attributes to others the ownership of companies, company shares or stocks or corporate offices, if the entrepreneur or company participates in procedures for the award or execution of contracts or concessions".

The following paragraph 10 of Article 3, Decree Law No 19 of 2 March 2024, on the other hand, amends the text of Article 84, paragraph 4, letter a) of the Anti-Mafia Code inserting, among the measures from which situations relating to attempts at mafia infiltration giving rise to the adoption of the anti-mafia interdictive information prohibition referred to in paragraph 3 of the same Article 84, also those that provide for a precautionary measure or judgement, or that result in a conviction, even if not final, for certain of the offences referred to in Articles 3 and 8 of Legislative Decree No. 74 of 10 March 2000. The amendment reflects, as observed here (p. 73) but also reported above by the Guardia di Finanza, the legislator's recognition that even the most serious tax offences – notably those involving the use and issuance of invoices for non-existent transactions and fraudulent declarations – are now committed, for the most part, by members of organised crime organisations, including mafia-type organisations and, therefore, useful elements for the application of preventive measures to curb attempts by criminal organisations to infiltrate the economy can also be derived from judicial measures concerning the offences themselves.

2.2.2. The role of complaints and reports by citizens and employees (the notion of "severe irregularity", conflict of interest and the whistleblowing regime)

Within the broader framework of protecting the European Union's financial interests, reports submitted by citizens, beneficiaries, and public employees constitute an increasingly significant source of information for the early detection of fraud, conflicts of interest (Del Gatto, 2024; Martines, 2022), and other irregularities involving EU funds.

In Italy, the first structured introduction of whistleblowing within the national legal system can be traced back to Law No 1906 of November 2012, the so-called "anti-corruption law", adopted with the aim of preventing and repressing illegality within the public administration (Mattarella, 2013). This law amended Legislative Decree 30 March 2001, No 165 by introducing an initial form of protection for employees who, by virtue of their employment relationship, become aware of unlawful conduct and report it to their hierarchical superior. Two years later, Decree-Law 24 June 2014, No 90, converted into Law 11 August 2014, No 114, assigned specific competences on whistleblowing to the National Anti-Corruption Authority (ANAC), thereby strengthening institutional oversight. A further and more substantial development occurred with Law 30 November 2017, No 179, which expanded the scope of application of whistleblowing in the public sector and identified the "Responsible for the Prevention of Corruption and Transparency" (RPCT) as the competent body for receiving and managing reports in place of the hierarchical superior. This reform also reinforced ANAC's role in supervising the system and ensuring the effective protection of reporting persons.

The legislative framework governing whistleblowing (see BETKONEXT Deliverable D1.3 and Deliverable D2.3) has undergone substantial consolidation, culminating in the transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, through Legislative Decree No 24 of 10 March 2023, which has strengthened preventive mechanisms, enhanced protections for reporting persons, and harmonised minimum standards across public bodies and private entities managing public resources.

Article 2 of Directive (EU) 2019/1937 explicitly includes breaches affecting the protection of the EU's financial interests. This scope is fully transposed into the Italian system through Article 2 of Legislative Decree No 24/2023, thereby ensuring that reports relating to fraud or irregularities involving Union funds fall within the harmonised safeguards framework (European Commission, 2024).

A key feature of Directive (EU) 2019/1937 is the significant expansion of the personal and material scope of whistleblower protection. From a subjective perspective, the Directive broadens the category of individuals eligible for protection to include not only public-sector employees but also private-sector workers. This extension reflects the recognition that unlawful practices affecting Union interests may arise across both sectors and that effective protection must embrace all individuals who can report such misconduct. From an objective perspective, the Directive expands the permissible subject matter of reports to cover breaches across a range of sectors considered economically, socially, and strategically significant to the Member States. Moreover, the Directive extends protection not only to reports of actual breaches but also to those based on **r**easonable suspicion, thereby ensuring that individuals are not discouraged from reporting information that, although not yet substantiated, may be crucial for the early detection of wrongdoing (Rubechini, 2024).

In this respect, also on the individual reporting side, the identification of situations of conflict and of symptomatic elements plays a crucial role in shaping the notion of a "suspected fraud", guiding reporting persons in recognising and signalling irregularities that may not yet amount to a fully ascertainable breach (paragraph 2.2.1). Article 2 of Legislative Decree No 24/2023 clarifies that a "violation" includes behaviours, acts or omissions that harm the public interest or the integrity of a public or private entity, including conduct that frustrates the object or purpose of Union provisions in the relevant sectors. The decree further defines "information on violations" as encompassing not only confirmed breaches but also well-founded suspicions based on concrete elements, as well as indications of attempts to conceal such conduct. This definition closely mirrors the concept of "information on breaches" set out in Article 5 of Directive (EU) 2019/1937, thereby ensuring full alignment between the Union's framework and its domestic transposition.

Reports from insiders or external stakeholders frequently provide the earliest indicators of new fraud schemes, especially where irregularities cannot be detected through standard administrative or automated controls; this is particularly evident in "new-generation" schemes

involving digital manipulation, fictitious corporate structures, or complex collusive arrangements, where insider knowledge is often the only effective means of identifying anomalies at an early stage. Legislative Decree No 24/2023 establishes a structured system of internal reporting channels, external channels managed by the National Anti-Corruption Authority (ANAC) and, under narrowly defined circumstances, public disclosure, which coexists with traditional mechanisms involving, at the European level, EPPO and OLAF (ANAC, 2023; Presidenza del Consiglio dei ministri, 2023).

In the Italian context, whistleblowing must also be understood within the broader context of administrative accountability (Donini, 2024). Reporting mechanisms constitute a crucial tool of "social accountability", enabling citizens and public employees to contribute to the oversight of administrative conduct and the protection of public resources. This function aligns with the principles of open government – transparency, participation, and integrity – by reinforcing the accountability and responsiveness of public entities involved in the management of EU funds. In this sense, whistleblowing does not merely support fraud detection but enhances the overall accountability ecosystem, thereby strengthening the safeguards surrounding the EU budget.

The domestic discipline introduced by Legislative Decree No 24/2023 ultimately reflects a faithful transposition of European law, conceived as a system of mutual support between the State and the reporting person. On the one hand, the State relies on whistleblowers to detect and diagnose anomalies that threaten the proper functioning of the administration and to safeguard public interests of a general nature. On the other hand, the reporting person relies on the State to prevent or remedy the adverse consequences that may arise from the act of reporting. The regime thus establishes a reciprocal relationship of protection and cooperation, in which the effectiveness of fraud prevention and the protection of individual rights are structurally interdependent (Rubechini, 2024).

In addition to reports submitted by employees or beneficiaries, an important complementary source of information arises from the anti-money laundering framework. Under Legislative Decree No 231 of 21 November 2007, obliged entities – including financial intermediaries, professionals and other regulated operators – must submit suspicious transaction reports to the Financial Intelligence Unit (UIF). These reports, based on anomalies in financial flows, may help detect conduct connected to fraudulent schemes or irregularities in the management of EU funds, including those related to the Recovery and Resilience

Facility. As highlighted in national AML analyses, STRs feed into a wider system of cooperation involving the UIF, the Guardia di Finanza and other competent authorities, thereby contributing to the timely identification of risks affecting the financial interests of the Union (Presidenza del Consiglio dei ministri, 2024).

In the management of EU funds – including cohesion policy instruments, the Recovery and Resilience Facility and programmes financed directly by the EU – whistleblowing, together with other reporting mechanisms such as suspicious transaction reports submitted under the anti-money-laundering framework, can be described as an important source of information for detecting irregularities, particularly in areas involving falsified or inaccurate expenditure documentation, undeclared conflicts of interest, ineligible or non-executed activities, and potential collusive behaviour in procurement or project selection. Despite ongoing challenges such as fear of retaliation, inconsistent implementation across administrations and limited awareness among potential reporters, Italy has introduced measures consistent with emerging good practices identified at EU level, including encrypted digital platforms, integrity-focused training, the integration of whistleblowing data into risk assessment and audit processes, and strengthened coordination among national authorities and OLAF. These developments intensify the detection of risks affecting the EU budget, particularly in a context characterised by increasingly complex, technology-driven fraud schemes.

2.2.3. The conventional network of the Guardia di Finanza safeguarding European financial interests

Protecting the financial interests of the European Union today represents one of the most significant junctions of cooperation between national and supranational legal systems, assuming a strategic role in ensuring the effectiveness of European policies and the legitimacy of public expenditure. In the multilayered architecture that safeguards the correct use of Union resources, Italy assigns to the Guardia di Finanza a peculiar and now structural function: that of an investigative-specialist body entrusted with ensuring, both preventively and repressively, the protection of the European budget according to the paradigm of the "equivalence" of protection standards established by Article 325 TFEU. The role of the Guardia di Finanza has progressively expanded in the transition from a model centred on the repression of fraud to an

integrated system of administrative cooperation capable of interconnecting information, documentary flows and operational activities of various national and European administrations.

From this perspective, the administrative cooperation carried out by the Guardia di Finanza is structured through a dense network of agreements, protocols, and conventions concluded with a wide range of national and European institutional actors. Indeed, the Guardia di Finanza has defined specific a forms of collaboration with all the subjects analysed below – each of which will be indicated in the paper with the full name and the related acronym in parentheses – creating an interaction model not limited to information exchange, but which affects the configuration of administrative processes of the control, risk assessment, and monitoring of European funds, including those related to the Recovery and Resilience Facility. This conventional dimension represents not only operational support but a genuine instrument of shared administration, aimed at strengthening the capacity of the Italian legal system to respond effectively to the obligations imposed by Union law and to prevent pathological phenomena such as fraud, embezzlement, and irregularities in the management of European resources.

From this perspective, the administrative cooperation carried out by the Guardia di Finanza is articulated through an extensive network of agreements, protocols, and conventions stipulated with a plurality of institutional actors.

Among the most relevant conventions are those concluded with the Ragioneria generale dello Stato (RGS) of the Ministero dell'economia e della finanza and with the Cassa Depositi e Prestiti (CDP).

On 17 December 2021, the Ministero dell'Economia e delle Finanze, together with the Guardia di Finanza, formalised a memorandum of understanding that is part of the broader institutional framework to ensure the full protection of the resources of the *Piano Nazionale di Ripresa e Resilienza* (NRRP). The agreement responds to the need to create an organic framework of cooperation capable of supporting, through a strengthened safeguard of legality and transparency, the implementation of an unprecedented investment programme in the history of the Republic. The transformative scope of the NRRP indeed makes indispensable a stringent, continuous, and multilayered model of administrative cooperation, consistent with the obligations imposed by the legal order of the European Union and with the expectations of efficiency and correctness that accompany the use of common resources.

It is Regulation (EU) 2021/241 itself, which established the Recovery and Resilience Facility at the European level, that precisely requires Member States to adopt all necessary measures to prevent and counter phenomena such as fraud, corruption, conflicts of interest and double funding, explicitly considered detrimental to the financial interests of the Union. This implies not only the activation of effective control systems, but also the strengthening and modernisation of the national anti-fraud system in all its components. In parallel, Decree-Law No 77/2021 outlined the national governance architecture of the NRRP, providing for the establishment, within the Ragioneria generale dello Stato and within the central administrations responsible for measures and investments, of bodies dedicated to oversight, audit, and monitoring. The same decree also recognised the power of these administrations to conclude memoranda of understanding aimed at strengthening interinstitutional cooperation; it is within this framework that the agreement with the Guardia di Finanza falls.

The centrality of the Ragioneria generale dello Stato is clear: it is the key coordinating body of the entire system, responsible for directing, coordinating, and supervising European financial flows, and for ensuring the proper use of resources. Complementary and essential is the role of the Guardia di Finanza, which, as the national economic-financial police force with general jurisdiction, is entrusted with preventing, detecting and prosecuting unlawful conduct capable of hindering the proper allocation of public resources to the programmed objectives. The interaction between the managerial, oversight, and control functions of the Ragioneria and the specific investigative expertise of the Guardia di Finanza translates, at the operational level, the European principle of equivalence of protection between national and Union funds.

The protocol is implemented through a particularly advanced system of information cooperation. It provides, in fact, for the pooling of a substantial body of data and information relating to the implementing, realising and executing entities of PNRR interventions, made possible by the interoperability of the databases of the two administrations. Such sharing does not constitute a mere documentary flow but feeds a dynamic risk-analysis mechanism that enables the timely detection of anomalies and directs control activities towards the areas of greatest exposure.

The agreement also governs the participation of the Guardia di Finanza in the "*rete dei referenti antifrode*", a coordination structure established within the Ragioneria generale dello Stato and composed of representatives of the same and of the central administrations responsible for the measures. Within this network, the periodic exchange of operational

experiences and the results of field inspections allows for increasingly precise identification of the sectors most vulnerable to fraud attempts, as well as the ex-ante calibration, in a preventive key, of the content of public calls and notices. The ability to intervene at an early stage in the investment administration cycle is one of the most innovative elements of the model outlined by the NRRP.

In this context, the protocol also provides for the possibility of scheduling operational activities to be entrusted to the Guardia di Finanza, to be carried out either autonomously or in coordination with the inspections conducted by the Ragioneria generale and the central administrations. This mode of cooperation, which integrates administrative functions with economic-financial police functions, enables faster responses to the emergence of critical issues and ensures timely, coordinated, and proportionate responses.

The memorandum, therefore, represents the expression of a shared strategy aimed at creating the conditions necessary for the vast resources of the NRRP to be used correctly, efficiently, and promptly, contributing to the full achievement of the growth, innovation, and resilience objectives set out in the Plan. The agreement is further distinguished in the European landscape because it explicitly and structurally provides for the involvement of a law enforcement body in the national PNRR control system: a distinctive element that enhances the role of the *Guardia di Finanza* as a specialised, stable, and qualified safeguard of economic and financial legality in the State.

Of great interest is also the more recent convention concluded between the *Cassa Depositi e Prestiti* (CDP) and the Guardia di Finanza. The Cassa Depositi e Prestiti (CDP) can be considered a public holding company under corporate law, insofar as it is a financial entity controlled by the State that performs functions of direction, coordination, and management of shareholdings in companies operating in strategic sectors for the country's economic development. In this capacity, CDP acts as the parent company of an articulated group of public or publicly participated enterprises, exercising governance, oversight and resource-allocation functions oriented towards the pursuit of public-interest objectives. Its nature as a public holding is characterised by the use of private-law instruments (shareholdings, financing, investments) for public purposes, through a hybrid model that combines market logic and institutional objectives, within the framework of European rules on State aid and public undertakings.

In April 2025, the convention between the Cassa Depositi e Prestiti and the Guardia di Finanza was signed, representing a significant component of the administrative cooperation system aimed at protecting the economic and financial interests of the State and the European Union. The agreement is indeed based on the objective of strengthening the effectiveness of the instruments of prevention, detection and countering of irregularities and fraud that may affect the correct management of public resources, including those of direct or indirect EU origin. The involvement of the Guardia di Finanza, as the national economic-financial police force with general jurisdiction, allows cooperation with CDP to be placed within the broader framework of measures required by European law to ensure an adequate level of protection of the EU budget, as established, among others, by Articles 310 and 325 TFEU, and by EU anti-fraud legislation.

The structure of the convention outlines an operational model in which CDP, consistent with its institutional functions of supporting enterprises, managing financial interventions and providing advisory services on projects of public interest, makes available to the Guardia di Finanza a structured flow of information designed to promptly detect anomalies, risks of criminal infiltration and possible fraudulent conduct. This flow concerns, in particular, the economic-support measures granted by CDP, the procurement procedures for works, services and supplies, and the interventions in which the company performs an advisory role: areas that, in practice, frequently overlap with projects financed or cofinanced by European funds, as well as with the investment lines included in the PNRR.

An element relevant to the protection of European financial interests is the provision of direct cooperation with the Nucleo Speciale Spesa Pubblica e Repressione Frodi Comunitarie, the specialised unit of the Guardia di Finanza dedicated to combating irregularities relating to EU funding. The convention thus enables the integration of CDP's internal expertise with the investigative capacity of the Guardia di Finanza, creating a qualified information circuit capable of supporting risk analyses, targeted insights, and operational interventions.

Particularly significant is also the possibility for CDP to report to the special units of the Guardia di Finanza the measures or contexts characterised by higher risk profiles, also in the light of its internal anti-money laundering assessments. In this way, preventive activity is not limited to a reactive dynamic but takes on an anticipatory character, consistent with the European approach that requires the adoption of early detection and risk-assessment tools for EU funds.

The convention also provides for the Guardia di Finanza's access to CDP's databases. This feature substantially enhances the Guardia di Finanza's ability to conduct cross-checks, trace financial flows, reconstruct corporate structures, and promptly identify potential fraud attempts or cases of double financing. This informational interoperability is fully aligned with OLAF guidelines, the reinforced-cooperation requirements set by Regulation (EU) 241/2021 on the Recovery and Resilience Facility, and national anti-fraud rules.

On a logistical and organisational level, CDP also undertakes to provide the Guardia di Finanza with the premises, tools, and materials necessary for carrying out the activities envisaged by the agreement, thus ensuring an operational environment suitable for the development of oversight and control functions. This aspect similarly contributes, indirectly, to reinforcing the safeguard of legality in the use of public resources, including European ones.

The model thus implemented, in cooperation with CDP, demonstrates that the protection of the EU budget depends not only on repressive tools but also on the construction of operational networks, the qualified sharing of information, and the activation of preventive procedures capable of promptly detecting anomalies and irregularities in the most exposed sectors.

The Guardia di Finanza has also concluded numerous other conventions, including with *Gestore dei Servizi Energetici* (GSE); *Ministero delle Imprese e del Made in Italy* (MIMIT); *Corte dei conti*; *Ministero delle Infrastrutture e dei Trasporti* (MIT); *Società per i Servizi al Mercato Agricolo Alimentare* (S.ME.A.); *Agenzia per le Erogazioni in Agricoltura* (AGEA); *Procura europea – European Public Prosecutor's Office* (EPPO); *Simest S.p.A.* (Simest); *Ministero dell'Ambiente e della Sicurezza Energetica* (MASE); *Istituto Nazionale della Previdenza Sociale* (INPS); *Dipartimento per l'Informazione e l'Editoria* della *Presidenza del Consiglio dei ministri* (DIE-PCM); *Ministero dell'Università e della Ricerca* (MUR); *Invitalia – Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa*; *Ministero della Cultura* (MiC); *Agenzia Nazionale per i Servizi Sanitari Regionali* (AGENAS); *Ministero del Turismo* (MiTur); *SACE S.p.A.* (SACE); *Società Infrastrutture Milano Cortina 2026 S.p.A.* (Milano-Cortina); *Dipartimento per le Politiche Antidroga* della *Presidenza del Consiglio dei ministri* (DPA-PCM); *Agenzia delle Entrate* (AdE); *Dipartimento per lo Sport* della *Presidenza del Consiglio dei ministri* (Sport-PCM); and *Dipartimento della Protezione Civile* (DPC).

The plurality and transversality of these conventions delineate a cooperation model that does not limit itself to information exchange but also affects the very structure of administrative

processes for control, risk assessment, and monitoring of European funds, including those of the Recovery and Resilience Facility. The conventional dimension of the Guardia di Finanza's activities thus constitutes an authentic instrument of shared administration, capable of strengthening the capacity of the Italian legal system to prevent fraud, irregularities, and embezzlement, and to comply effectively with the obligations imposed by Union law.

3. Belgium

3.1. Belgium: Institutional Context and Fraud Oversight

Belgium is a federal State, and its complex institutional structure makes it unique among EU Member States, including in protecting European Union financial interests. The country is composed of two types of federated entities: Communities and Regions. There are three Communities, based on language and culture: the Flemish Community, which includes Dutch-speaking inhabitants of the Brussels-Capital region; the French Community, which includes French-speaking inhabitants of the Brussels-Capital region; and the German-speaking Community. In addition, there are three territorial Regions: the Flemish Region, the Walloon Region, and the Brussels-Capital Region (Vlaamse Regering, n.d.). Certain policy areas, such as education, rural development, and the protection of EU financial interests, fall under regional jurisdiction.

The competences of each region and of the federal level are explained in detail in the Special Act concerning the Reformation of the Institutions (Bijzondere Wet tot Hervorming van de Instellingen) and the Constitution. Despite this formal division of powers, conflicts may occur due to the inherently complex nature of Belgium's institutional arrangement.

Given this dispersed institutional structure, protecting EU financial interests requires effective coordination among multiple national authorities and with EU bodies such as OLAF and the EPPO. To ensure coherent oversight and effective cooperation across these actors, Belgium has designated the Anti-Fraud Coordination Service (AFCOS), which operates within the Federal Public Service Economy, as the central coordination mechanism. AFCOS acts as the secretariat of the national AFCOS network and serves as the main contact point for OLAF.

Importantly, the role of AFCOS in Belgium is fundamentally coordination-oriented, facilitating communication, cooperation, and information exchange among the wide range of competent authorities involved in protecting the EU's financial interests.

More specifically, AFCOS's competences include:

- raising awareness among the relevant stakeholders (e.g., regional authorities) about the protection of EU financial interests

- acting as the first contact point for OLAF in the event of information or data requests, which are typically managed through the AFCOS secretariat
- providing support in matters falling within OLAF's remit, for example, by supplying bank account details or following up on issues involving EU staff
- providing (fraud prevention) training

The next part of this working paper draws primarily on the interview with a representative of the Belgian AFCOS, written input from a representative of the Belgian tax authorities, and desk research. These discussions provide examples of actual cases and highlight the practical obstacles and limitations that authorities face in protecting EU financial interests, including coordination challenges involving multiple authorities, legal barriers, etc.

3.2. Expenditure Monitoring of EU Support Funds

According to the interview with AFCOS representatives, financial statement and project management issues frequently arise in EU-funded research and institutional projects. Common problems include incomplete documentation, underreported work, and cases where personnel are officially listed as participating in projects but do not perform the related tasks. Missing or incomplete time sheets further complicate the verification of expenditures, illustrating the challenges of ensuring that funds are used appropriately. Similar difficulties have also been identified in regional development projects. These challenges are evident in real-life cases.

Case Example: Lacs de l'Eau d'Heure (Wallonia, Belgium)

The Lacs de l'Eau d'Heure project in Wallonia, which received EU support for regional tourism development, illustrates the monitoring challenges and implementation risks associated with EU-funded initiatives. Following a complaint regarding project management, OLAF conducted a preliminary assessment and, in coordination with AFCOS Belgium, carried out an on-the-spot check. The investigation focused in particular on the equestrian centre, valued at nearly €2 million and partly financed by European funds.

Inspectors requested access to administrative and financial documentation at the project's headquarters in Falemprise to assess compliance with EU funding rules. Initially, the ASBL (a non-profit organisation), responsible for the Lacs de l'Eau d'Heure, described the OLAF visit as a routine inspection. However, during a parliamentary commission hearing in autumn 2024, the Walloon Minister for Tourism, Valérie Lescrenier, clarified that OLAF had opened a formal procedure nearly two years earlier concerning the management of EU funds for the equestrian centre. The Commissariat General for Tourism had submitted relevant documents and had been interviewed twice by OLAF representatives (RTBF, 2024).

According to the AFCOS representative, the investigation confirmed indications of potential fraudulent activity, demonstrating that the scrutiny was not merely procedural but aimed at detecting misuse of European funds.

The ASBL managing the Lacs de l'Eau d'Heure project received EU funding, including €400,000 for an equestrian centre. However, no operator has been found despite several calls for interest. EU rules require that funds be used for their intended purpose; if the centre is repurposed, the funds must be reimbursed (RTBF, 2024).

RRF Funds Oversight

AFCOS plays a central role in monitoring the Recovery and Resilience Facility (RRF) funds; it also assisted in creating the entire RRF framework at the federal level.

Its responsibilities include coordinating on-the-spot verifications, advising, and consulting on potential fraud risks. It provides guidance and training to various authorities, such as the inspection of finance (main audit authorities in Belgium), on fraud, fraud prevention, conflicts of interest, corruption, and double financing.

AFCOS ensures that reported project outputs and activities are consistent with reality during these on-site checks, helping to detect discrepancies and prevent misuse of funds. Usually, the project integrity evaluation is performed by checking whether the beneficiaries' reports correspond to reality.

During inspections, for instance, in case of an infrastructure project, AFCOS may review technical documentation, verify infrastructure works, examine financial records, and ask project staff for clarifications to confirm compliance with subsidy agreements. Routine checks frequently uncover discrepancies between declared outputs and actual project

activities, enabling timely corrective actions, such as suspending funds or implementing additional oversight.

Effective implementation of these checks poses a significant challenge. It requires not only expertise in finance and project management but also highly specialised knowledge of the technical standards, regulatory frameworks, and operational realities of a particular sector. Evaluating complex infrastructure or research projects demands an understanding that goes beyond administrative oversight, encompassing engineering specifications, environmental requirements, or scientific methodologies. This need for multidisciplinary and sector-specific expertise makes oversight resource-intensive and operationally complex, but essential for safeguarding EU financial interests.

3.3. VAT and Customs Fraud

While the previous sections focused on EU expenditure, protecting the EU's financial interests also requires robust oversight of revenue-side fraud, particularly VAT and customs cases.

Protecting the EU's financial interests in Belgium involves not only administrative oversight but also criminal oversight, for example, in cases of VAT and customs-related fraud.

In criminal matters affecting the EU's financial interests, including VAT fraud, the EPPO plays a central role. However, as highlighted in the previous working paper, national authorities in Belgium remain important actors: investigating judges may still lead certain intrusive investigations, and designated officials from the customs administration cooperate with EPPO prosecutors to investigate and prosecute customs-related offences. This highlights again the importance of close coordination between the EPPO and Belgian national authorities to ensure the effective investigation and prosecution of VAT and customs-related offences.

According to an AFCOS representative, Belgium faces elevated risks of VAT and customs-related fraud due to the high volume of goods entering through its air and sea ports.

Limited inspection capacity and staff shortages further reduce the likelihood of detection, creating vulnerabilities in the import control system.

This assessment is consistent with insights from a representative of the tax inspectorate, who confirmed that VAT fraud, customs fraud, and related carousel schemes occur on a large scale in Belgium.

A representative from the tax authorities highlighted that e-commerce has become particularly susceptible to both VAT and customs fraud. This area presents a growing challenge for the Belgian authorities. Some major market actors operating in the digital marketplace contribute little or nothing to the national economy – paying neither customs duties, VAT, nor direct taxes – despite generating substantial revenues from EU consumers. The complexity and transnational nature of online transactions make it difficult to trace financial and logistical flows, illustrating how new forms of digital commerce can undermine the protection of the Union's financial interests. These risks materialised in several major operations, including the well-known "Silk Road" case.

Case Example: The "Silk Road" Operation (2023)

On 28 March 2023, the European Public Prosecutor's Office (EPPO) carried out ten searches in several locations across Belgium, including Liège Airport. It arrested four suspects in an operation against a customs fraud ring believed to have caused up to €310 million in losses in evaded taxes and customs duties. The operation, conducted with the support of Europol, Belgian Customs and VAT authorities, and various branches of the Belgian Police, involved raids on storage premises and offices at Liège Airport and in Zeebrugge, as well as private homes in Ans (Alleur), Liège, and Visé. Authorities seized documentary evidence and assets, including electronic devices and company records.

The investigation, code-named *"Silk Road"*, targeted Chinese exporters suspected of establishing a complex system to evade VAT on imported goods. According to the EPPO, the scheme operated through three Belgian private customs agencies acting as reliable representatives for the exporters, and a network of fictitious companies across several EU Member States. The companies falsely declared that goods entering the EU through Liège Airport–such as electronic devices, toys, and various consumer accessories – were destined for

other Member States, thereby benefiting from a VAT import exemption under the EU's *Customs Procedure 42 (CP42)* (EPPO, 2023).

This mechanism enabled the perpetrators to avoid paying VAT and customs duties in Belgium while selling products in the EU market, thereby creating substantial illegal profits. The case underscores the risks associated with inadequate customs oversight in major logistics hubs such as Liège and Zeebrugge, as well as the challenges of controlling high volumes of e-commerce imports.

It is important to note that serious VAT fraud in Belgium, particularly cases affecting the financial interests of the EU, can result in imprisonment of up to 5 years and fines of €2,000–€4,000,000 (Careel & De Smedt, 2022).

Case example:the 'Kingdom' case (2024)

A cross-border investigation led by the EPPO, code-named 'Kingdom', involved a Belgian subsidiary of a Dutch company that submitted fraudulent VAT refund claims to the Belgian Treasury based on fake invoices. The Treasury initially paid out €13.7 million to several bank accounts controlled by the suspects. However, the scheme was detected when one of the banks flagged suspicious transactions and returned €3.7 million to the Treasury, preventing part of the fraud. Investigations revealed that no actual goods were traded, and the VAT claims were unlawful. The suspects, who were already known to Dutch authorities for similar offences, attempted to replicate the scheme with another Belgian branch of a Dutch company. (EPPO, 2024).

The case illustrates the cross-border nature of VAT fraud and the need for close coordination among competent authorities, involving the Belgian Treasury, the Belgian Federal Police, the Dutch Fiscal Information and Investigation Service (FIOD), the Dutch Public Prosecutor's Office, and EPPO. Investigative measures included joint searches in Belgium and the Netherlands, highlighting practical mechanisms for cooperation across Member States.

Both cases reveal that VAT and customs fraud in Belgium commonly relies on cross-border structures, the use of shell or fictitious companies, and the manipulation of EU procedures such as CP42 or VAT refund mechanisms. Fraudsters often exploit logistical hubs like Liège and Zeebrugge, together with intermediaries, to disguise illegitimate transactions.

These schemes highlight systemic vulnerabilities in customs oversight, VAT controls, and cooperation across Member States.

3.4. Tools and Challenges in Detecting and Investigating EU Financial Irregularities

Whistleblowing is a legally protected mechanism in Belgium for reporting serious wrongdoing, including fraud and corruption. As highlighted in our previous working paper, the Belgian law provides protection to whistleblowers reporting breaches in several areas of EU law, including public procurement, financial services, and transport safety.

The law provides three ways to make a disclosure:

- Internal reporting: reporting the issue within the organisation concerned
- External reporting: contacting the competent authorities designated by law (e.g. the Federal Ombudsman)
- Public disclosure: communicating the issue through the media or online, but only in exceptional cases (FIRM–IFDH, 2025)

Recent data show that, in practice, a large share of whistleblower reports concern social fraud rather than fraud directly linked to EU financial interests or large-scale financial misconduct. According to the 2024 annual report of the Federal Ombudsman, in the private sector, half of the reports concerned social fraud, while the remainder addressed issues such as public health, fiscal fraud, financial services, market- or product-related problems, and data protection.

Although the law establishes formal safeguards, the sharp rise in anonymous reporting – particularly in the private sector (from 65 cases in 2023 to 146 in 2024) and, to a lesser extent, in the public sector (from 9 to 12) – suggests that whistleblowers perceive anonymity as a crucial form of protection against retaliation (Federal Ombudsman, 2024).

Despite the legal framework, there are still no clear indicators that whistleblowers in Belgium benefit from strong and effective protection. This may discourage individuals from reporting concerns, especially in cases involving financial or institutional wrongdoing.

Whistleblowing represents only one part of Belgium's broader fraud-detection landscape. In practice, irregularities involving EU funds are identified mainly through a set of

administrative, technological, and operational tools used by authorities and investigative bodies.

According to the AFCOS representative, Belgium employs a combination of technological, administrative, and on-site tools to detect and investigate fraud involving EU funds:

- Risk-scoring tools: The ARACHNE tool is widely used to identify potentially high-risk projects financed by EU funds. At the Flemish level, the CATE tool complements ARACHNE by strengthening fraud detection and risk management
- Integrated Management System (IMS): Some indications of potential irregularities are flagged through IMS, which collects and monitors project data and financial flows, enabling early detection
- On-the-spot checks: Authorities conduct inspections at project sites to verify whether reported activities and expenditures correspond to actual implementation.
- Administrative audits and document review: Financial statements, invoices, contracts, and other project documentation are examined to detect inconsistencies or anomalies.

The Fraud Control Department plays a central coordinating role in ensuring these tools are used effectively through training. It provides a structured framework for conducting enquiries, emphasising the identification of relevant stakeholders who need to be informed or involved when a potential irregularity is detected. For example, when a suspicious transaction is flagged – whether through IMS, ARACHNE, or other sources – appropriate authorities are notified to ensure a coordinated response. This framework supports efficient information-sharing, timely interventions, and a clear chain of responsibility among all actors involved.

However, the effective use of these tools is constrained by a number of systemic challenges which hinder the effective detection and prosecution of fraud affecting the EU's financial interests in Belgium.

- One of the main challenges is the limited communication between competent authorities at both national and EU levels, which can delay the timely sharing of information relevant to fraud detection and investigation

- Resource constraints represent another significant obstacle. Investigations into EU fund fraud often demand highly specialised expertise in areas such as finance, technical project management, or sector-specific regulations. Limited staffing and budgetary resources can make it difficult to manage these complex and resource-intensive cases efficiently
- Legal and procedural barriers add another layer of difficulty. Certain legislative requirements or multi-layered administrative procedures – such as ratification processes for inter-institutional agreements – may unintentionally slow down cross-authority cooperation, affecting the speed and effectiveness of fraud detection.
- The technical complexity of emerging sectors, such as digital commerce, green transition initiatives, and advanced infrastructure projects, further complicates oversight. Verifying compliance in these areas requires not only general administrative knowledge but also an in-depth understanding of sector-specific norms and standards.
- In addition, language and cultural challenges in Belgium's multilingual environment can be an obstacle to smooth collaboration among authorities. A further consideration is the perception of reporting: suspicions of fraud are sometimes seen as administrative failure rather than an essential part of risk management, which may discourage timely reporting.

Emerging trends in fraud also reflect broader technological and geopolitical developments. Artificial intelligence (AI) is increasingly deployed to support investigations, enabling authorities to analyse large datasets and identify complex networks of fraudulent activity. At the same time, fraudsters are also leveraging AI to create sophisticated schemes and falsified data, introducing new challenges for detection and prevention. Intelligence-led approaches are becoming more common, in which sectoral mapping – such as for telecom projects or green transition initiatives – helps identify potential vulnerabilities proactively. Geopolitical shifts, such as increased defence spending and evolving supply chains, may also introduce new risks, including price manipulation, monopolistic practices, or cross-border irregularities that require close monitoring.

These structural, operational, and emerging vulnerabilities underscore the need for continuous adaptation, coordination, and investment in Belgium's fraud-detection and

prevention mechanisms, ensuring that authorities can respond effectively to current and future threats to EU financial interests.

3.5. Conclusion

Belgium's complex institutional architecture shapes both the strengths and the vulnerabilities of its system for protecting the European Union's financial interests. The dispersion of competences across federal, regional, and community levels makes coordination essential, and AFCOS plays a central role in ensuring communication and coherence across the multiple authorities involved. Its work – particularly in training, awareness-raising, and managing exchanges with OLAF – constitutes a clear best practice within a fragmented governance system.

However, the insights gathered through interviews and case studies reveal structural challenges that continue to hinder effective oversight. In the area of EU expenditure, recurrent issues such as incomplete documentation, underreported work, and discrepancies between reported and actual project activities point to persistent weaknesses in project management and monitoring. The Lacs de l'Eau d'Heure case illustrates how these weaknesses can escalate into suspected fraud, demonstrating the need for more robust verification methods and timely cooperation among competent actors.

In the domain of VAT and customs fraud, Belgium's position as a major logistics hub magnifies exposure to large-scale carousel schemes, e-commerce-related fraud, and abuses of customs procedures. The "Silk Road" and "Kingdom" cases show that these schemes are both highly sophisticated and inherently cross-border, requiring deep cooperation with EU bodies such as the EPPO, as well as with foreign tax and customs authorities.

Belgium employs a range of tools – ARACHNE, CATE, IMS, audits, and on-the-spot checks – that contribute significantly to the early detection of irregularities. Yet their effectiveness is constrained by recurring obstacles: limited communication flows between authorities, shortages in specialised staff, complex legal and procedural requirements, and the expertise needed to oversee increasingly specialised and technologically advanced projects.

Overall, the Belgian experience demonstrates that safeguarding EU financial interests requires sustained engagement in coordination, expertise, and prevention mechanisms.

Strengthening stakeholder management – knowing which authority to involve, when, and how – remains essential in a multi-layered system where responsibilities are widely dispersed. At the same time, AFCOS's training activities and emphasis on awareness-raising show that building a shared understanding of fraud risks across institutions remains crucial. Ultimately, the central driver behind these efforts is the protection of EU citizens and consumers, whose interests depend on the integrity, transparency, and proper use of public funds.

4. Spain

4.1. Introduction

This chapter examines the detection and investigation of fraud and corruption cases in Spain, with particular attention to protecting the European Union's financial interests.

To this end, Section 2 presents recent cases of fraud and corruption in which, either conclusively or on credible indications, the financial interests of the European Union may have been affected. The analysis is structured in two groups: (2.1) cases concerning VAT fraud, and (2.2) other corruption and fraud cases. Each group comprises two cases, for a total of four cases under review.

These cases are of relative significance, as they have prompted reflection on their potential impact on the Union's financial interests, and at least one of them has, notably, attracted recent media attention. In addition to outlining each case and its possible European dimension, the chapter offers several forward-looking considerations to guide potential improvements aimed at strengthening fraud and corruption prevention.

Section 3 addresses two key issues: (3.1) the effectiveness of whistleblowing channels in Spain–one of the principal mechanisms for detecting fraud and corruption – and (3.2) the national anti-corruption plan of July 2025.

The first issue is highlighted because whistleblowing remains the primary mechanism for detecting breaches of the law, particularly in cases involving fraud or corruption. Furthermore, the Spanish State has upheld the relevance of whistleblower-protection legislation as a means of safeguarding the Union's financial interests (see section 2.26.2 of the Report on Measures adopted by the Member States to protect the EU's financial interests - Implementation of article 325 TFUE, SWD(2025) 228 final). However, its still very limited practical application suggests that Spain faces substantial challenges in effectively achieving the objectives set out in Directive (EU) 2019/1937.

The second issue, the national anti-corruption plan, was presented by the Government of Spain in July 2025 with a degree of urgency, as a firm and immediate response to the public disclosure of an alleged and serious corruption case involving public-works contracting in

which, among others, a former government minister is implicated by actions made during his period as Transport Minister (case included in section 2.2). At this stage, the national plan remains only as a plan, and its measures will need to be further developed, approved, and implemented. Nevertheless, it constitutes a notable step forward that merits inclusion in this report, as it is relevant in Section 2.2 to describe the events that prompted the need for a more robust response to corruption and fraud in Spain.

Lastly, Section 4 summarises several of the main conclusions of the workshop held at the University of Barcelona on 19 September 2025, within the framework of the Betkonext project. The workshop underlined, inter alia, the centrality of whistleblowing channels (noting that, in Spain, AFCOS operates a reporting channel for fraud affecting the use of EU funds) and the growing importance of digital tools capable of detecting patterns or indicators of fraud or corruption.

4.2. Recent Cases of Fraud and Corruption

4.2.1. Fraud against the financial interests of the European Union through the abusive application of VAT regulations

4.2.1.1. Analysis of VAT fraud and the protection of the European Union's financial interests: current situation

In accordance with Article 325(1) and (2) of the Treaty on the Functioning of the European Union, the Union and the Member States must combat fraud and any other illegal activities affecting the financial interests of the Union. To this end, it will be necessary to take all measures necessary to deter Union citizens from engaging in such conduct and to be able to offer effective protection in the Member States and in the institutions, bodies, and agencies of the Union. In this regard, Member States are required to establish a comparable level of protection to prevent fraud affecting financial interests at the internal and European level.

When we refer to the financial interests of the European Union, we are referring not only to budgetary allocations intended to support strategic areas – such as regional

development, agriculture, scientific research, infrastructure, or any other area of intervention by the European institutions – but also to the set of resources that feed into and consolidate the common budget. The latter includes revenue from customs duties on imports from third countries, the proportion of value added tax that Member States contribute to the European coffers and various additional financing mechanisms. Together, these elements form the financial architecture that enables the European Union to implement its policies, promote economic and social cohesion, and effectively address the structural and cyclical challenges within its sphere of action. These resources therefore become a fundamental tool for delivering on promises of progress, cohesion, and social justice.

Specifically, this contribution will focus on the second dimension, namely the mechanisms for obtaining resources and, in particular, the role of Value Added Tax (VAT) in financing the Union. VAT fraud is, in fact, one of the most significant ways in which the financial interests of the European Union are undermined, not only because it directly reduces the revenue that Member States must make available to the common budget, but also because it distorts the functioning of the internal market, alters competition, and weakens confidence in the integrity of the European tax system. Studying this issue is therefore central to understanding the current vulnerabilities of the EU financing model and identifying the reforms needed to strengthen its sustainability and its ability to respond to increasingly sophisticated illegal practices.

Among the most widespread schemes of fraud against the financial interests of the European Union – and therefore the one on which we will focus– is the so-called carousel fraud, or Missing Trader Intra-Community Fraud. This mechanism exploits the benefits of the tax regime for intra-Community trade in goods to evade VAT, setting up a chain of apparently legitimate transactions across different Member States to avoid paying this tax. Essentially, these illegal transactions involve several companies purchasing goods in another European Union country without being required to pay tax at the time of purchase. They then introduce these goods into the domestic market of another Member State, apply the corresponding VAT, and, in a final stage, disappear without declaring or remitting the collected taxes to the tax authorities. In many cases, these schemes resort to using front companies or newly established companies – created specifically for this purpose – to dilute responsibilities, cover the tracks of operations, and impede the work of tax authorities.

In this regard, it should be noted that carousel fraud within the European Union is not a minor problem, as VAT evasion has had and continues to have an enormous economic impact and directly affects the availability of funds needed to finance public administrations and services. The loss of resources undermines states' ability to invest in health, education, infrastructure, and social policies, and also generates unfair competition that harms companies that comply with their tax obligations. By way of reference, in 2022, European Union Member States lost around €89 billion in revenue due to this type of fraudulent practice, which always involves avoidance schemes, administrative errors, or VAT payment insolvencies. This significant gap between what should theoretically have been collected and what was actually collected by the tax authorities highlights the magnitude of the problem and the need to study this issue in greater depth.

In Spain, the estimated losses for that same year amounted to around €4.443 billion, equivalent to a 4.59% shortfall in total revenue. These figures not only illustrate the scale of fraud, but also the difficulty of controlling its spread in an increasingly dynamic and digitalised cross-border trade environment.

These practices not only involve a reduction in public revenue but also generate side effects that directly affect the functioning of the internal market and social cohesion. On the one hand, competition between companies is distorted, as those that strictly comply with their tax obligations are at a clear disadvantage compared to those who, through fraud, can offer artificially lower prices or illegally increase their profit margins. As a result, the rational functioning of the internal market is undermined, as transparency and trust in public institutions are reduced, honest investment is discouraged, and it may even lead to the exclusion from the market of those operators or entrepreneurs who, acting legitimately, are unable to compete on equal terms.

Furthermore, fraud against the financial interests of the European Union, and in particular carousel fraud, weakens the financing of public services, as every euro that does not enter the State coffers represents a reduction in the resources available for the necessary maintenance of our welfare state model and hinders the provision of some essential public services, such as health, education, infrastructure and social policies. The continued loss of this revenue forces public authorities to make budgetary adjustments to align their spending capacity with their needs, which ultimately affects the quantity and quality of services available to citizens.

Finally, eradicating such abusive practices is necessary to ensure public perception of tax justice. When society observes that certain economic actors can evade their tax responsibilities with impunity, a sense of dissatisfaction arises, undermining confidence in European and national institutions and in the very logic of the tax system. Ultimately, this loss of legitimacy can foster attitudes of disaffection and reduce taxpayers' willingness to voluntarily comply with their tax obligations, creating a vicious circle that jeopardises the sustainability of the tax system.

4.2.1.2 Carousel fraud or Missing Trader Intra-Community Fraud

Carousel fraud is one of the most widespread mechanisms of VAT tax evasion. Specifically, this type of fraud exploits current regulations on intra-Community acquisitions of goods, as they do not require VAT on such acquisitions to be paid immediately. These goods are then sold to shell companies, whose managers often disappear before filing and paying their respective VAT returns. In this regard, it should be noted that there is no single form of carousel fraud; rather, these practices have become highly sophisticated.

This type of fraud can be carried out in the context of intra-Community acquisitions of goods, defined in Spanish legislation in Articles 13 et seq. of Law 37/1992 of 28 December on Value Added Tax. In these cases, a business owner from one Member State purchases goods in another Member State without incurring the obligation to pay VAT in the country of origin and is required to self-assess this tax in their own quarterly return. This special regime contrasts with the system provided for imports of goods from third countries, where the importer must declare and pay VAT directly at customs. This means that, in intra-Community trade, these goods can be moved to another Member State without having to pay tax and without being subject to this prior control regime.

If we analyse this fraud scheme in more detail, we see that, in these cases, missing trader companies usually purchase large volumes of goods without paying VAT and immediately sell them at very low prices to so-called broker companies located in the same Member State or another. The key is that in this first sale, the missing trader company charges VAT on the invoice issued to the broker company. At this point, the second company already has an invoice with input VAT that can be deducted, and, at that very moment, the missing trader company is

obliged to declare and pay the tax. However, this first company disappears before doing so, meaning that these amounts are not paid into the public coffers.

In turn, in this type of fraud, it is common to use so-called buffer societies, which act as intermediaries in the criminal chain between the missing trader companies and the broker companies. Their function is to introduce an additional barrier that gives the appearance of commercial normality and complicates the investigation. These companies purchase the goods from the missing trader, also taking advantage of the intra-Community acquisition regime and, in many cases, at prices well below market value. Then, these companies resell them almost immediately to a broker society, which will close the transaction and request a refund of the VAT paid.

The involvement of these buffer societies does not correspond to any real economic activity, but rather to a deliberate strategy to complicate the traceability of transactions and dilute the responsibilities of those who commit these offences. By multiplying the number of participants and transactions, it becomes more difficult for public authorities to reconstruct the commercial flow, track tax accruals, and identify the main beneficiaries of the fraudulent activities. Ultimately, their creation is intended to hinder detection and prosecution by the tax and judicial authorities, increasing the complexity and opacity of the organised scheme.

Regardless of the sophistication of the operations carried out within the framework of carousel fraud, the intended objective is always the same, namely to ensure that the broker company has a valid invoice showing that it has paid the VAT corresponding to the goods, so that, subsequently, when marketing those goods and submitting tax returns, it can claim the deductions provided for in the regulations.

4.2.1.3 Recent cases of carousel fraud in the Spanish legal landscape

By way of example, and in order to contextualise the relevance that this phenomenon is acquiring in Spain (Cáceres, 2024), it is worth noting that, so far this year alone, the Spanish tax authorities, in collaboration with the European Public Prosecutor's Office, have launched investigations into two particularly serious cases. These operations have resulted in the arrest of forty individuals, which demonstrates not only the magnitude of the criminal network but also the growing organisational capacity and sophistication of the networks involved. These

figures highlight the real scale of the problem and underscore the need to strengthen prevention, control, and institutional cooperation mechanisms to tackle a phenomenon that continues to evolve and adapt to existing supervisory measures.

In the first of these cases, for which the most recent updates came in January of this year, the Spanish law enforcement authorities, acting under the direction of the European Public Prosecutor's Office (EPPO) in Madrid, dismantled a transnational criminal network involved in the sale of luxury vehicles through a scheme specifically designed to evade the payment of VAT. The organisation operated through a complex structure of shell companies and fictitious transactions, enabling high-end cars to be placed on the Spanish market without fulfilling the corresponding tax obligations. The estimated financial damage in Spain alone exceeds €17 million, a figure that highlights both the scale of the fraud and the sophistication of the methods employed to obscure financial trails and hinder investigative efforts.

According to the investigation, the head of the criminal organisation, based in Germany, was responsible for coordinating the scheme remotely by issuing instructions for the supply of vehicles to various car dealerships in Spain. From German territory, the vehicles were channelled through two operational branches of the network, each one responsible for organising their transport and ensuring their correct delivery to the Spanish dealerships (the broker societies). These intermediary branches played a crucial logistical role, enabling the seamless movement of cars across borders while concealing the illicit nature of the transactions and facilitating subsequent VAT evasion.

A third branch of the organisation is believed to have been responsible for constructing the complex corporate and transactional framework necessary to carry out the VAT fraud and to launder the illicit proceeds it generated. This part of the network allegedly designed and managed a system of "missing traders" and shell companies, entities created solely to avoid VAT payments by disrupting the audit trail and obscuring the true nature of the operations. These companies, often short-lived and lacking any genuine economic activity, were instrumental in sustaining the façade of legitimacy around the scheme, enabling the criminal network to conceal both the origin of the vehicles and the flow of funds, and thereby ensuring that the profits derived from the fraudulent activity could be reintegrated into the legal economy with minimal risk of detection.

Furthermore, this case was regarded as particularly serious due to the methods employed by the organisation. According to the evidence gathered, the criminal network

recruited vulnerable individuals to serve as “straw men” for the shell companies used in the fraudulent scheme. These individuals–often in precarious social or economic situations–were placed as front directors or shareholders in exchange for basic accommodation in properties owned or controlled by members of the organisation. By doing so, the perpetrators not only shielded themselves from legal responsibility but also deepened the opacity of the corporate structure, making it significantly more difficult for investigators to identify the actual decision-makers.

Another recent case, made public in July of this year, resulted in the dismantling of a major criminal organisation specialising in large-scale VAT fraud in the alcoholic beverages sector. According to preliminary findings, the group is believed to have orchestrated an extensive scheme to evade VAT on commercial transactions spanning several fiscal years. Between 2018 and 2024 alone, the organisation is estimated to have incurred tax losses of nearly €69 million.

This criminal organisation maintained extensive international connections and, for years, specialised in refining schemes targeting the financial interests of the European Union and the Spanish Public Treasury. Its operations in the alcoholic beverages market were conducted through a complex corporate structure composed of 93 companies registered in Spain, Portugal, Germany, Malta, and the Turks and Caicos Islands. In parallel to this network, the organisation also controlled an auxiliary corporate framework through which the proceeds of its illicit activities were channelled and subjected to sophisticated money laundering procedures.

In both cases, carousel fraud techniques were used. Spanish shell companies were utilised to simulate the direct acquisition of goods and merchandise from suppliers located in other EU Member States, through intra-Community acquisitions subject to the general VAT regime, which justified the original exemption from VAT. Subsequently, these introducing traders sold the products to other Spanish entities–the distributor companies–charging VAT on the corresponding invoices. However, the introducing traders failed to submit their VAT obligations for those sales, while the distributor companies nevertheless deducted the same VAT, even though it had never been paid by the original operators. This mechanism of tax evasion enabled distributors to market goods at substantially reduced prices, benefiting from the artificial margins generated by prior VAT fraud.

Furthermore, in the first of the cases studied, it was found that the criminal organisation had designed a simulated chain of transactions to acquire vehicles from foreign shell companies, with the aim of altering the applicable VAT regime and thereby hindering the detection of the fraud. More specifically, these entities received invoices subject to the standard VAT regime for intra-Community supplies of goods which, under the applicable legislation, were exempt from the tax. They then unlawfully altered the applicable tax regime by issuing invoices to the Spanish distributor entities under the special scheme for second-hand goods, which is incompatible with the nature of the underlying transactions as defined by law. Through this fraud mechanism, the Spanish distributors were formally enabled to issue invoices to their own clients under the special scheme for second-hand goods. This, in turn, led those clients – and ultimately the entire downstream distribution chain – to apply this more favourable tax regime in their subsequent sales. The result was a substantial, artificial reduction in VAT liability throughout the commercial chain.

These two cases served as a paradigmatic example of the crucial role of European cooperation in addressing offences that, by their very nature, transcend national borders. Carousel fraud represents one of the most serious and persistent threats to the financial interests of the European Union. Its impact on public finances is particularly significant, as it systematically undermines the income that constitutes a major source of revenue for both Member States and the EU budget.

Given the inherently cross-border nature of carousel fraud–characterised by networks of shell companies, simulated transactions, and the rapid movement of goods across Member States–effective responses must go beyond traditional, nationally confined approaches. No single country can confront these schemes in isolation. This reality underscores the need to strengthen administrative cooperation, modernise and harmonise VAT control mechanisms, and reinforce the role of institutions such as the European Public Prosecutor's Office (EPPO), which has proven essential in coordinating the investigation and prosecution of crimes affecting the financial interests of the Union.

4.2.1.4 The insufficient response of the Spanish legal system to carousel fraud

In Spain, concerns about providing an adequate response to VAT fraud date back at least to 2008, with the approval of the Spanish Government's Tax Fraud Prevention Plan. This document proposed, on the one hand, the necessity of introducing mechanisms to enforce joint liability for the payment of tax obligations, targeting the various operators involved in carousel fraud chains, following the example of several European Union Member States, such as the Netherlands, the United Kingdom, Germany, Austria, and Italy. These countries have implemented a set of measures that have proven to be an effective tool in deterring criminal organizations from participating in fraudulent schemes. On the other hand, the possibility of restricting or cancelling access to the Register of Exporters and other Economic Operators was considered for those taxable persons who request VAT refunds when such refunds appear to derive from transactions linked to carousel fraud schemes. This measure was designed as a preventive mechanism to avoid the deduction of artificially generated tax liabilities.

In addition, the document proposed conducting a detailed analysis of current cases of reverse charge to assess their real effectiveness in the fight against carousel fraud and to evaluate the possibility of extending their scope to other sectors or scenarios where this type of fraud frequently occurs.

Finally, it assessed the need to implement regulatory changes to prevent tax refunds from being issued to taxpayers who had resorted to chaining together successive transactions to conceal VAT fraud. The proposals ranged from automatically converting such refunds into amounts to be offset to imposing stricter guaranteed requirements, forming a comprehensive approach aimed at minimising the economic incentives that encourage the proliferation of these criminal structures.

In this regard, within the provisions contained in Spanish law, one of the principle rules for mitigating the impact of carousel fraud and, in general, tax evasion in relation to unpaid VAT, is the subsidiary liability regime provided for in Article 87 of Law 37/1992 of 28 December on Value Added Tax, introduced by Law 36/2006 of 29 November on measures to prevent tax fraud. This provision is the main tool available to domestic tax authorities to discourage voluntary or negligent participation in fraudulent transaction chains. The application of this provision allows certain economic obligations to be imposed on those who,

due to their position in the transaction, benefit from artificially reduced prices or fail to exercise the required diligence. Through this instrument, the legislator aims to strengthen the integrity of the VAT system and ensure that economic operators act with the reasonable prudence necessary to detect and avoid participation in schemes such as carousel fraud, which seriously affect the financial interests of the European Union and its Member States.

The provision establishes a regime of subsidiary liability applicable to certain recipients of VAT-taxable transactions, to strengthen the protection of the public Treasury against fraud, especially that linked to opaque or irregular marketing chains. In general terms, it is determined that entrepreneurs or professionals who acquire taxable goods may be held subsidiarily liable for VAT not paid by those who carried out such transactions, provided that, given the circumstances of the specific case, they should reasonably have presumed that the tax charged would not be declared and paid by the person responsible. It is, therefore, a mechanism that penalises the lack of diligence in economic transactions and requires those involved in them to exercise a minimum standard of caution when establishing their commercial relationships.

This article outlines the circumstances under which the tax authorities may extend the obligation to satisfy unpaid amounts to distribution companies. Specifically, the existence of payments at "notoriously abnormal prices" for the goods purchased must be verified. This notion is configured as an objective indicator that should alert the purchaser to the possibility of irregularities in commercial transactions. A price is considered notoriously anomalous in two cases: when the price paid is significantly lower than what would correspond to similar goods under normal market conditions, or when it is significantly lower than the purchase price paid by the transferor. In both cases, the clear price difference allows us to infer that the acquiring company should have noticed the irregularity and, therefore, cannot claim good faith or ignorance of the underlying tax fraud.

To classify the price as abnormal, the tax authorities must carry out a rigorous analysis, taking into account both the available documentation and the documents provided by the distributing company. Where possible, they will also compare the disputed transaction with other transactions carried out in the same economic sector that are highly similar. This comparison enables the determination of the market value at the time of the transaction, which serves as a benchmark for assessing whether the price paid deviates unjustifiably from normal economic parameters.

Finally, for this subsidiary liability to be enforced, the Administration must prove that VAT was charged but not declared or paid by the taxpayer obliged to do so. Subsidiary liability, in accordance with Spanish regulations, is not automatically presumed simply because of an anomalous price, but requires proof of prior tax non-compliance. The aim is to prevent the purchasing company from obtaining an undue advantage or contributing, either fraudulently or negligently, to fraudulent practices that erode tax collection, thereby strengthening the effectiveness of the tax system and the fight against illegal structures such as those frequently used in carousel fraud.

The effectiveness of the above provision has been significantly reinforced by developments in European and Spanish case law, which has consolidated the existence of a duty of enhanced diligence on the part of businesses when operating in the internal market. Both the Court of Justice of the European Union and the Spanish courts have held that economic operators cannot remain passive in the face of reasonable indications of fraud in their supply chains, particularly in sectors exposed to carousel fraud. Thus, it has been stated that businesses must take measures, such as verifying the identity and reliability of their suppliers, checking for abnormally low prices, or analysing the regularity of transactions, to ensure that the VAT charged has been, or will be, correctly declared and paid. This line of case law complements and strengthens the subsidiary liability provided for in domestic legislation, creating a framework that requires taxable persons to play an active role in preventing and detecting fraudulent practices in intra-Community trade. In this regard, we can mention the consolidated case law of the Supreme Court, among others, in its ruling of 14 January 2013, which states that “an orderly and diligent trader must, in his own interest, check the characteristics of the traders with whom he establishes commercial relations. This knowledge must be particularly thorough, the more intimate and frequent those commercial relations are”.

4.2.2 Other Fraud and Corruption Cases

First of all, it is highly relevant to note that, during the preparation of this report, news broke of the first conviction in Spain resulting from a trial in a case investigated by the European Public Prosecutor’s Office (EPPO). Previously, all convictions had stemmed from plea agreements. The news published on 18 July 2025 states that a company and two of its

legal representatives were convicted of fraud totalling €3.8 million related to agricultural subsidies. The conviction imposes a one-year prison sentence on each of the two defendants, a €3 million fine on each, and a €3 million fine on the company. The company is also required to repay €2 million in unlawfully obtained funds.

The fraud originated when the company applied for and obtained a subsidy in 2018, subsequently breaching the conditions by seeking additional financing incompatible with the initial aid. The initial subsidy from the Spanish Agricultural Guarantee Fund (FEAG) was granted to improve its facilities used for the production of fruit and vegetables. Later, the defendants also applied for loans from the Catalan Finance Institute and the Directorate-General for Industry [here].

This case illustrates the need for interoperability of subsidy registries – or their eventual centralisation – as well as the opportunity to jointly develop data-analysis tools capable of identifying cases of double financing among Member States (and their regions and local bodies that award subsidies). The development of the Arachne system, together with the prospect of requiring its use and proper data input by Member States, is therefore pertinent and of great value.

The second case presented is currently highly prominent in the Spanish media, was uncovered in recent months, and is still generating news as the judicial investigation progresses to clarify the facts. It concerns the irregular awarding of construction contracts linked to the Ministry of Transport. Since this is an ongoing investigation, the information available is still insufficient to describe the case in great detail, but at least two elements of the alleged corrupt scheme can be outlined on an indicative basis: the operation of the allegedly irregular awarding of contracts in favour of companies that paid bribes, and the alleged concealment of the funds derived from those bribes.

It should also be noted that it has not yet been established whether or not there is any damage to the financial interests of the European Union. On the one hand, available information suggests that some construction works financed with EU funds may have been affected by the corrupt scheme, such as the railway station in the municipality of Sant Feliu de Llobregat. The contract notice stated the following: “II.2.13. Information on European Union funds. The contract relates to a project or programme financed by European Union funds: Yes. Project identification: It may be co-financed by the Connecting Europe Facility (CEF).” [here].

However, on the other hand, in response to a request from the European Public Prosecutor's Office, in October 2025, the investigating judge of the court clarified that, so far, there is no evidence that the construction projects under investigation have involved EU funds, although this possibility cannot be ruled out. Nonetheless, the judge pointed out that this factor may be of little significance, since the purpose of the case is to examine the possible existence of criminal organisations that allegedly obtained public works contracts through bribery and the suspects' influence, regardless of the funds used in those projects [here].

Originally, at the end of 2024, an investigation had been opened into a scheme involving the collection of bribes related to the purchase of medical supplies – mostly face masks – during the COVID-19 pandemic, under urgent and emergency procedures [here].

The judicial case, however, took a turn in June 2025, expanding suspicion of corrupt practices to the former Minister of Transport himself, the organisational secretary of the governing political party in the Spanish Government, and high-value public works contracts. As stated by the investigating judge of the Supreme Court in his Order of 3 November 2025 (ECLI:ES:TS:2025:10280A) (originally written in Spanish, translated into English here):

"On 5 June 2025, the Central Operative Unit of the Guardia Civil, the economic investigation and anti-corruption department attached to the Special Prosecutor's Office against Corruption and Organised Crime (hereinafter, U.C.O.), submitted a police report which contains, essentially, though not exclusively, information on the possible unlawful awarding of public works, within the Ministry of Transport–primarily through ADIF and the Directorate-General for Roads–in exchange for certain financial rewards. This report, which includes, among other relevant elements, indications arising from the telephone and computer devices seized from Mr ___ during the search of his home (ordered at the time by Central Investigating Court No. 2), reflects the possible involvement of Mr ___, a member of parliament at the time, as well as that of other persons linked to construction companies and other public officials, with precise identification of some of the public works that may have been the object of such allegedly illicit awards."

In another Supreme Court Order, issued in September 2025 (ECLI:ES:TS:2025:8919A), the court indicates that the alleged *modus operandi* could have involved influencing the procurement procedures for public works tendered by the public company ADIF, through the Director-General for Roads, with the involvement of the President of ADIF, so that the company that had paid (or promised to pay) the bribe would be awarded

the contract despite not having submitted the best bid. To achieve this, the subjective-assessment criteria of the bids were allegedly overvalued:

"The UCO officers, after considerable analytical effort, were able to identify in their report the specific public works apparently awarded in each of the localities referred to so explicitly in the conversations. In all of them, a common element was identified: the works were awarded to the aforementioned company (ACCIONA CONSTRUCCIÓN in a joint venture with smaller companies), whose financial offer was not, in any of the cases, the objectively preferable one, but which benefited from the decisive subjective assessment under the chosen award procedure. Various WhatsApp or email communications were also seized between Mr ___ and the Director-General for Roads or the President of ADIF, or with individuals acting in the interests of the favoured construction companies, explicitly referring to the award procedure of the different public works. It is also important to note that there is clear–once again, only on an indicative basis–evidence of Mr ___'s links to the company SERVINABAR, 2000, S.L.U., which had already been awarded certain works, prior to Mr ___'s appointment to the Ministry, acting precisely in a joint venture despite its minimal size and lack of experience in the construction business, together with ACCIONA CONSTRUCCIONES." Thus, one of the methods by which the bribe may have been channelled was through payments between the two companies forming the joint venture for the tender.

In the light of this case, and based solely on conjecture until a final judgment is issued, one could conclude that the lack of experience of a small company within a joint venture–partnered with a very large and clearly solvent company able to carry out the works without the assistance of the inexperienced one–could be a risk indicator for possible corruption in public contracts. Moreover, the fact that an offer in a public procurement procedure is ranked first under subjective award criteria should also be considered a red flag. Indeed, there may well be legitimate reasons for a better offer to outperform others in aspects subject to subjective assessment, but since the evaluation of such criteria is an area of risk in procurement, significant alterations in the prioritisation of bids should receive special audit attention, and the officials responsible for subjective assessment should be warned of the risks inherent in their tasks.

4.2.3 Special references: the problems presented by the Spanish law on the protection of whistleblowers and the anti-corruption measures plan, of July 2025, presented by the Spanish Government

4.2.3.1. Whistleblowing Law (Law 2/2023)

Law 2/2023, made in Spain, transposed the Directive (EU) 2019/1937. Both legal regimes aim to foster a culture of legality by making reporting breaches of the law safe and easy, prohibiting reprisals, and establishing protection mechanisms for reporting persons. The Spanish Law is yet to be developed by regional law, with details on the specific implementation of the whistleblowing framework in each Autonomous Community.

The Spanish Law 2/2023 is unclear in some areas, and there is considerable uncertainty about its implementation (Capdeferro, 2025). For example, one issue that has generated widespread concern among experts, as it may be contrary to the Spanish constitutional and legal system, is the limitation of remedies in relation to information reported (Parajó Calvo, 2023: 103-104).

These articles provide that, internally, decisions adopted by public bodies with auditing or investigative functions in relation to reported information may not be appealed either administratively or in administrative-contentious proceedings, and the same applies to decisions taken by the protection authority concerning the conclusion of investigative proceedings on received reports.

On this regulation, authors such as Ponce (2025:127) or Carbajo (2023:149-150) have suggested that it may be unconstitutional insofar as it limits the right to appeal, and in particular Carbajo has indicated that this regulation creates areas in which the actions of administrative bodies are unchecked and removed from jurisdictional control, which is incompatible with the rule of law and would require the ‘resolute’ intervention of the Constitutional Court.

Another critical problem is the fact that, under article 35 of the Law 2/2023, reporting persons could be excluded from protection on some wide causes: when it concerns information contained in communications that have been inadmissible through any internal or external channel; when the information refers to interpersonal conflicts; when the information is already in the public domain or is merely a rumour; and when the actions or omissions reported are not within the regulatory scope of Article 2. Only focusing on the first cause for exclusion of the protection and support measures, it may be added that there is no closed list of grounds for inadmissibility in the internal channels. In contrast, the law provides one for the external channel in Article 18.2. a). In consequence, it could be seen as an excessive margin for limiting protection, since, even if the report is accepted by the external channel, if it was previously submitted and rejected by an internal channel, the whistleblower would be left unprotected in the event of reprisals.

However, in this report we will focus in one problem that could be considered against the Directive. The major problem that arises in relation to the correct transposition is, in our opinion, the time limit on protection against reprisals. According to Law 2/2023, protection against reprisals would, in principle, extend for a maximum period of two years, since it specifies that protection beyond two years is exceptional and may be granted, where applicable, in a justified manner by the competent protection authority upon request (art. 36.4 of Law 2/2023). In fact, this time limitation has been described as one of the most criticized aspects of the law: “This aspect, the limitation of protection for victims to two years, has been one of the greatest criticisms of the Law”, noting that “people who report corruption face reprisals for years” (Subirana de la Cruz & López Donaire, 2023:167).

Trying to justify this two-year limitation is somewhat complex, as it stems from inconsistent decisions during earlier stages of the legislative process, since, as I will now explain, it should not have appeared even in the bill submitted by the Government.

Originally, Article 36(2) of the Draft Law regulating the protection of persons reporting regulatory infringements and combating corruption limited the concept of reprisal to those practices that occur “while the investigation procedure is ongoing or within the two years following its conclusion or the date on which the public disclosure took place”. However, paragraph 4 of the same article allowed, albeit with an error regarding the time period (referring to one year instead of the two mentioned above), for the protection to be exceptionally extended.

Opinion 1361/2022, of 8 September 2022, issued by the Council of State regarding this draft bill, states that the directive being transposed by this future law establishes no time limitation for protection against reprisals. Therefore, this temporal restriction should be removed, and the opinion points out that the justification provided in the file is purely budgetary, meaning it lacks any legal basis:

"However, there are other differences that are indeed objectionable. The first lies in the fact that Article 36(2) of the draft bill introduces a time limit for protection against reprisals that is not foreseen in any way in the Directive, by establishing the condition that 'such acts or omissions occur while the investigation procedure is ongoing or within the two years following its conclusion or the date on which the public disclosure took place'. The file shows that this time limitation is a legislative policy option motivated by budgetary considerations, since 'an indemnity or aid system cannot be established indefinitely'. This, however, is not a valid reason to justify departing from the text of the Directive on this point, since the European rule protects, in principle, against all types of reprisals that meet the three requirements of Article 5(11), regardless of whether they occur before, during or after (even years after) the investigation procedure".

The Council of State, however, considers that a time limitation could indeed appear– possibly to address the budgetary concern, but only with regard to financial and psychological support measures:

"It should be recalled, however, that the provision of the financial and psychological support measures set out in Article 37(1)(c) of the draft bill could, in principle, be time-limited, given that their implementation is purely optional for Member States under Article 20(2) of Directive 2019/1937".

The Council of State, in the light of the above, requests, as an essential observation, the removal of the time limitation in Article 36(2), relating to the definition of reprisal. However, it seems to overlook that the same "time limit for protection against reprisals, which is not foreseen in any way in the Directive", reappears in paragraph 4, and it does not request its removal.

As shown in the Regulatory Impact Assessment Report for the Law regulating the protection of persons who report regulatory infringements and combat corruption, dated September 2022, the Government did indeed remove the wording with the time reference in Article 36(2). However, because the Council of State had not specifically addressed the same

time limitation in paragraph 4 of the same article, the final version of the bill–and later the enacted law–retains the clause allowing protection to be exceptionally extended beyond two years.

Consequently, *sensu contrario*, it must be understood that the clause that should have been eliminated continues to apply, since ordinarily. Unless the protection authority expressly grants a time extension, after two years, there will no longer be a right to protection.

Unfortunately, this partial removal of the time limit leaves the remaining limiting clause incomplete, as it is no longer clear which time period Article 36(4) refers to, or when that period begins (Pérez Monguió, 2023:269-273).

At this point, given that the directive establishes no time limit, it is difficult to understand how a provision whose content, as the Council of State has already pointed out, is contrary to the directive could be interpreted as conforming to it. It therefore seems necessary to remove this time limitation–either by amending Law 2/2023 on this point, or by designing the regional transposition legislation with the aim of fully complying with the directive, overcoming the limitation imposed by the national law. Ideally, both Law 2/2023 and the regional implementing legislation should dispense with this time limitation.

4.2.4 National Anti-Corruption Plan of July 2025

Following the outbreak of a serious corruption case involving possible bribes linked to irregular contract awards, the President of the Spanish Government presented the so-called National Plan to Combat Corruption, dated 9 July 2025. The plan further indicates that it will need to be complemented by the implementation of the national anti-fraud strategy, which has not yet been approved. However, the plan states that its adoption is expected before the end of 2025.

According to the aforementioned State Plan, on page 10, it states that it fulfils “the commitment undertaken in the 2023 Whistleblower Protection Act, which required us to develop a strategy to strengthen the fight against corruption”. This reference to Act 2/2023 appears in the Fifth Additional Provision, which indicates that the Government, “within a maximum period of eighteen months from the entry into force of this Act, and in collaboration with the Autonomous Communities, must approve a Strategy against Corruption, which must

at least include an assessment of compliance with the objectives established in this Act, as well as any measures deemed necessary to address the shortcomings identified during this period". It should be assessed whether, despite the deadline having been missed (as more than two years have passed since the Act 2/2023 entered into force), this plan at least satisfies the other elements required by the Fifth Additional Provision, such as collaboration with the Autonomous Communities or the proper inclusion of the content elements prescribed.

In any case, given that some of the strategic statements of intent contained in the plan refer to matters addressed in the previous section, it seems appropriate to briefly mention them. Specifically, the plan–structured around five thematic pillars–dedicates the second pillar to the effective protection of persons who report irregularities and cases of corruption (whistleblowers). Among other elements mentioned, such as a possible reform of the Criminal Procedure Act, the following proposals may be highlighted as undoubtedly interesting and aligned with the solution to some of the many problems identified previously: the power of the competent authorities to directly nullify acts of retaliation; and the recognition of managers of internal and external reporting channels as protected persons, "including an extension of their protection for five years after the end of their functions" (p. 20).

The remaining thematic pillars are referred to as the following topics.

The first pillar focuses on preventing corruption in order to reduce its incidence. Among the planned measures, the central one is the proposal to create an Independent Agency for Public Integrity as the main body responsible for preventing, supervising, and prosecuting corruption. In our view, the plan proposes to broaden and deepen risk-management measures already implemented during the execution of the Next Generation funds, extending the use of integrity risk maps to all public funds and adopting a systemic, preventive approach. This pillar also highlights the importance of digitalisation in combating corruption in public procurement, proposing to transform the Public Sector Contracting Platform through Big Data and Artificial Intelligence to prevent corruption. The third pillar focuses on measures related to investigating, prosecuting, and sanctioning corruption. Among other measures, it includes the creation of specialised anti-corruption and public administration offences sections within the new instance courts, strengthening the Anti-Corruption Prosecutor's Office with additional resources and personnel, and assigning the Public Prosecutor's Office responsibility for directing criminal investigations, granting it greater autonomy and transparency.

The fourth pillar is dedicated to the recovery of assets derived from corrupt activities as an essential element in repairing the harm caused to the public interest. The main measure under this pillar is likely the strengthening of the Asset Recovery and Management Office, the body within the State Administration responsible for assisting judicial bodies and prosecutors in locating, among other things, profits derived from corruption. This office was created in compliance with Directive 2014/42 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union and must, by November 2024, be adapted to the provisions of Directive (EU) 2024/1260 on asset recovery and confiscation.

Finally, the fifth pillar focuses on promoting an anti-corruption culture among citizens, businesses, and public administrations through training, social campaigns, and surveys on perceptions of corruption. Among other measures, it includes the development of mandatory training programmes and the dissemination of best practices in integrity and corruption prevention for public-sector staff, as well as the organisation of a social campaign to strengthen anti-corruption awareness and inform the public about the need for and the possibilities of reporting irregularities in public institutions.

The implementation of the plan will therefore need to be closely monitored to see when and how the measures outlined in the plan are eventually materialised and codified, but the measures proposed seem appropriate and could yield positive effects in the fight against fraud and corruption.

4.2.5 Conclusions of the 19 September Workshop at the University of Barcelona, “The protection of the EU’s financial interests: tools and practices for prevention, detection and investigation”

On 19 September 2025, the Seminar titled “The protection of the EU’s financial interests: tools and practices for prevention, detection and investigation” took place at the University of Barcelona. This seminar was an activity of the Betkonext project, aimed at sharing current issues, interests and concerns related to the protection of the Union’s financial interests in Spain. The event included participation from national (Spain and Italy) and regional authorities, as well as the project’s researchers.

In general terms, the seminar addressed issues related to preventing fraud and corruption, and detecting cases that could not be avoided or prevented.

Regarding prevention, the main instrument highlighted was the anti-fraud measures plan for the prevention and management of fraud, corruption and conflict-of-interest risks. Such plans are required in Spain for public administrations to manage subsidies and public contracts financed with EU NextGeneration funds, pursuant to Order HFP/1030/2021 of 29 September, which establishes the management system for the Recovery, Transformation and Resilience Plan.

The representative from the European Funds and State Aid Office of the Department of Economy and Finance of the Government of Catalonia explained that these plans have been designed in practice in line with national recommendations and based on the application of risk methodologies. They have been complemented with relevant instruments such as conflict-of-interest declarations, risk indicators (red flags), a channel for reporting irregularities, and a code of ethics.

Additionally, she indicated that the anti-fraud measures plan within the regional government of Catalonia provides that, as soon as a possible breach is detected in a public procurement or subsidy procedure related to European funds, the procedure is immediately suspended. The file is reviewed at an early stage, in order to minimise as far as possible the impact of potential irregularities. In this regard, this early corrective reaction may be seen as a good practice, provided that it is efficient and effective.

Concerning the preventive measures implemented, the training and awareness-raising efforts could be highlighted as good practices. In particular, the representative of the Catalan European Funds and State Aid Office noted that they had held eight workshops at the regional level and provided online training to local entities, and that they had collaborated with the School of Public Administration of Catalonia and the Anti-Fraud Office of Catalonia in the design of specific trainings on the implementation of the regional Catalan anti-fraud measures plan and the approval of local entities' plans.

Regarding the detection of fraud and corruption cases, the Head of the Data Analysis Team of the Anti-Fraud Office of Catalonia and the State Comptroller and Auditor in the European Funds Division (General Intervention of the State Administration), both participating in the seminar, stressed the importance of digital tools and data analysis to improve fraud-detection capabilities.

The Head of the Data Analysis Team at the Anti-Fraud Office of Catalonia presented the progress made in developing their new data analysis tool to monitor the proper use of public funds. For the moment, the tool has been tested and developed mainly for application in the control of public procurement (still in the development phase), and some red flags that have successfully been implemented in the system were presented, such as the following: detection of potential conflicts of interest in public procurement proceedings; abuse of non-competitive public procurement proceedings (buyer side); contract splitting through minor contracts (small-value contracts) using direct awarding procedures; single-bidder proceedings; potential intervention of the future winner in the preliminary preparation of the procurement procedure (technical specifications/terms of reference metadata); linked companies (same address/representative). Despite being a digital tool still under development, the results obtained during the testing and design phase have been promising. Consequently, it appears to be good practice to invest efforts and resources in designing and refining support tools for detecting fraud and corruption cases, such as this system developed by the Anti-Fraud Office of Catalonia or the European Commission's Arachne system. It could also be proposed that information exchange and collaboration between public institutions be improved, as it currently appears that each institution or body is developing its own systems independently and, without connection or interoperability, even though they often aim to detect similar types of breaches.

On the other hand, the State Comptroller's representative explained the use and operation of the national red-flags tool, Minerva. The Minerva System was introduced in Spain through Order HFP 55/2023 to analyse and detect potential conflicts of interest between decision-makers and beneficiaries in public procurement and subsidy procedures involving EU Next Generation funds. The red flags of this system include situations in which the decision-maker is the potential beneficiary, the real owner of the potential beneficiary, or its administrator, or a director or member of the board of directors of the potential beneficiary. It also detects cases where the decision-maker is a first- or second-degree relative of the potential beneficiary, or when there are commercial transactions between the decision-maker and a real owner of the potential beneficiary. When one of these red flags is detected, the procedure must be stopped to assess whether the decision-maker concerned should refrain from participating.

Given the tool's use, it might be considered good practice to design digital tools that enable access to data stored in databases at different points in time. For example, if analysing a case from two years ago, it should be possible to work with the data as it existed at that time,

as indications of a conflict of interest might be found in past data that no longer appear in present datasets.

Regarding case detection, the other element highlighted by the speakers–besides digital tools–was the whistleblowing channels. These were emphasised by the representative of the Spanish AFCOS (National Anti-Fraud Coordination Service) and the representative of the Independent Authority for Whistleblower Protection.

The Spanish AFCOS representative highlighted its coordination and cooperation functions and emphasised the specific investigative functions it carries out. Specifically, they highlighted the role of their whistleblowing channel, through which they can identify potential cases for investigation. It is a confidential channel for reporting breaches that harm the financial interests of the European Union. Once a breach is confirmed, AFCOS may issue recommendations regarding the detected irregularity, monitor compliance, and refer the case to the competent authority for possible sanctions. The main issue highlighted by the speaker was the large number of existing reporting channels and the difficulty of cooperation and coordination, as complaints regarding the same facts may be submitted through multiple channels, leading to several parallel investigations without clear competence delineation or coordination mechanisms in cases where multiple channels could be appropriate for reporting the same issue.

The representative of the Independent Authority for Whistleblower Protection emphasised the importance of fostering a culture of legality and the crucial role that authorities responsible for protecting whistleblowers must play in strengthening it. In Spain, this system is divided between regional authorities and the national authority, and it will be critical that the national authority, through the coordination and cooperation mechanisms foreseen in the law, ensures an adequate standard of protection across the national territory and promotes good protection practices. Also worthy of note as a good practice is the proposal by the representative of the Independent Authority to provide training to public employees through the National Institute of Public Administration, as well as the development and application of nudging techniques to promote respect for whistleblowers and the culture of legality. However, several challenges were identified, such as the need for sufficient budget and staff, and the need for connection to external national and European channels.

The seminar also featured participation from the Italian AFCOS (whose contribution was particularly valuable, as it enabled dialogue with the Spanish AFCOS) and the group's

researchers, whose presentations addressed key aspects of the protection of financial interests in various countries, each from the perspective of the respective speaker. Their conclusions highlighted the need to advance cooperation and to jointly develop solutions to address similar, often transnational problems.

5. Poland

5.1. Introductory remarks

Poland is one of the countries where protecting the European Union's financial interests is significant, given the scale of European funds inflows and the complexity of the institutional structures responsible for their expenditure. A review of available analyses reveals that violations of the EU's financial interests in Poland are multidimensional, encompassing both traditional financial fraud and new forms of fraud related to digitalisation and technological development. The most frequently identified irregularities include bid rigging, falsification of project documentation, overstatement of eligible costs, sham partnerships in research and innovation projects, e-commerce fraud, and manipulation of the actual scope of tasks performed. Some of these abuses are organised and indicate deliberate exploitation of weaknesses in management and control systems.

Against this background, the initiated overhaul of the Polish system for combating corruption and financial fraud may be a significant turning point for the future effectiveness of protecting the EU's financial interests in the country. The proposed changes include the abolition of the Central Anti-Corruption Bureau and the reformulation of the anti-corruption policy coordination model by strengthening the role of the Prime Minister, creating an anti-corruption protection mechanism and increasing the involvement of institutions such as the Police, the Internal Security Agency and the National Revenue Administration in tasks related to the detection and prevention of fraud. This reform aims not only to eliminate previous dysfunctions but also to create a more transparent, cooperative, and functional institutional architecture, adapted to the growing complexity of threats.

The conclusions of the scientific seminar on the responsibility of collective entities and the protection of the EU's financial interests emphasised that the effectiveness of the anti-fraud system in Poland depends on the State's ability to control not only the activities of individuals, but above all the organisations and institutions that are the main administrators of EU funds. It was noted that many abuses are structural, rooted in organisational procedures rather than in individual actions. Therefore, the development of effective mechanisms for the accountability of collective entities, despite its dogmatic difficulties, is an important element in strengthening

the protection of EU funds. The importance of better coordination between national institutions, the development of analytical tools and the raising of transparency standards in the public sector was also emphasised.

The chapter on Poland will therefore focus on reviewing the most important types of fraud in the area of EU funds, analysing the evolution of Poland's national anti-corruption and anti-fraud system, and assessing the challenges Poland faces in the context of reforms aimed at increasing the financial security of the State and the European Union.

5.2. Protecting the EU's financial interests in Poland: Case law

Below are three cases of fraud affecting the EU's financial interests in Poland that, due to their nature or importance, warrant presentation. One case concerns the expenditure of EU funds and is politically charged, as it has sparked a heated public debate over their rational allocation. At the same time, the speed of the government's, the control authorities', and law enforcement agencies' responses shows that suspicions of EU money being wasted are being taken seriously. The second case, on the other hand, reveals a complex mechanism of international VAT fraud involving many entities from different EU countries. It is also an example of the importance of cooperation between EU authorities and national authorities, as well as cooperation between Member States.

Expenditure Case law: the KPO scandal in the HoReCa sector

In August 2025, Polish public opinion was heated by a scandal surrounding KPO funds allocated to the HoReCa sector. Support from the KPO was intended for companies that suffered the most during the COVID-19 pandemic and experienced a year-on-year turnover decline of at least 20% in 2020 and 2021. The subsidies aimed to modernise or diversify the companies' activities to make them more resilient to future crises. Poland received money from the EU Recovery Fund much later than other Member States, only in 2024. (here). The delay in the disbursement of funds was due to a conflict over the rule of law between the previous United Right government and the European Commission. The release of these funds in exchange for promises to carry out appropriate reforms, the so-called milestones, is one of the

greatest successes of Prime Minister Donald Tusk and the so-called 15 October Dinner. In August 2025, the list of beneficiaries and the allocation of subsidies were disclosed. Due to the nature of the industry and the assumed goal of diversification, many applicants requested, for example, the purchase of yachts (e.g. if someone ran a hotel or restaurant, a yacht was to be a diversification of conventional activities, so as to offer, for example, rental in the event of another lockdown), saunas, solariums, virtual shooting ranges, coffee machines, or even swingers' clubs, etc. The nature of these purchases attracted public attention, as the purchase of saunas or yachts may seem extravagant, and the opposition took advantage, launching a campaign attacking the government for squandering EU money.

As part of the support for the HoReCa industry, a total of 3,005 contracts worth PLN 1.2 billion were concluded under the KPO, i.e. less than half a per cent of the total value of the KPO for Poland (here). Prime Minister Donald Tusk promised to audit every zloty spent and to report any irregularities requiring criminal prosecution to the law enforcement authorities. The President of the Polish Agency for Enterprise Development (PARP), responsible for conducting the competition, lost her position. Initially, the investigation into the matter was taken up by the Regional Prosecutor's Office in Warsaw, which, after a few days, referred it to the European Public Prosecutor's Office. In the second half of September 2025, the results of the first audits were released, revealing 16 cases of irregularities. As a result, six contracts were withdrawn, and funding worth almost PLN 3 million was cancelled. The Ministry of Funds and Regional Policy carried out 12,000 audits of subsidies granted to entrepreneurs from EU funds since 2021, of which 1,159 concerned the NRP itself. In the projects checked from all funds allocated for 2021-2027, the irregularity rate was 1/10, and in the case of subsidies from the KPO, this rate was 0.005% (here).

Case law: VAT fraud

In 2025, a sophisticated VAT fraud scheme involving goods imported from China to the European Union was uncovered in Poland. OLAF worked on the case in collaboration with Polish tax and customs authorities in Poland, Germany, the Czech Republic, Lithuania, and Latvia. OLAF uncovered a complex network exploiting the so-called "Customs Procedure 42", a mechanism that defers VAT payments on goods imported into one Member State and subsequently transported to another. Criminals operating as part of an organised criminal group transported goods from China to Germany via a railway border crossing under the customs

transit procedure, suspending customs duties and VAT. Upon arrival in Germany, the goods were declared under procedure 42 and then transported back to Poland and stored in warehouses near Wólka Kosowska (here). Wólka Kosowska is a specific place in Poland, known to law enforcement agencies and the National Revenue Administration (KAS) and Border Guard, where numerous companies, often completely fictitious, are based, most often with foreign capital, mainly Vietnamese, Chinese and Turkish. Wólka Kosowska is a centre for the wholesale trade in counterfeit goods, and the entities operating there, in addition to crimes against industrial property, are often also involved in money laundering or tax fraud. In the case under analysis, the imported goods were allegedly exported by front companies registered to citizens of Lithuania, Ukraine and Russia to other EU countries, mainly Lithuania. However, in reality, they remained in Poland or were illegally distributed within the EU, including to Germany, Spain, France, and Italy.

This practice enabled the avoidance of VAT, resulting in significant illegal profits. OLAF forwarded the information to the Regional Prosecutor's Office in Krakow, which is conducting criminal proceedings in this case. In April 2025, Polish authorities, including officers from the Internal Security Agency (ABW), the National Revenue Administration (KAS), the Central Bureau of Investigation (CBŚP) and the Central Bureau for Combating Cybercrime (CBZC), carried out arrests and searches. Close cooperation between OLAF and national authorities, as well as cooperation between Member States, makes it possible to uncover cross-border crimes, VAT fraud, to the detriment of the EU's financial interests (here).

Poland's involvement in the work of the EPPO

Another case worth mentioning, given that it is already being investigated by the EPPO and concerns abuses by high-ranking officials, including the mayor of Nowy Sącz and his deputy, concerns public procurement. In October 2025, the European Public Prosecutor's Office applied a preventive measure in the form of suspension from official duties of, among others, the officials indicated, who were alleged to have manipulated a public procurement procedure in order to obtain an undue financial advantage of EUR 600,405 (PLN 2.6 million) for the Sądecka Agencja Rozwoju Regionalnego S.A. (here).

5.3. The (un)certain future of the CBA. The government is liquidating it, and the opposition is protesting

5.3.1. Introductory remarks

On 21 November 2025, the Sejm decided to begin work on a draft law concerning the liquidation of the Central Anti-Corruption Bureau [Print No. 1884. Government draft bill on the coordination of anti-corruption measures and the liquidation of the Central Anti-Corruption Bureau. Dostęp on-line here]

. The reform providing for the liquidation of the Central Anti-Corruption Bureau (CBA) is one of the most significant projects to restructure Poland's internal security system and institutional anti-corruption infrastructure since the service's establishment in 2006. The explanatory memorandum to the draft law presents a comprehensive, multifaceted picture of the institutional crisis in which the CBA finds itself, as well as a model for combating corruption that relies on a specialised service with extensive operational powers that may infringe upon civil rights.

The document indicates that the reform is not a technical measure but a response to systemic, legal, political, and social problems that undermine citizens' trust in the State and its ability to pursue an effective and impartial anti-corruption policy. The explanatory memorandum begins with the statement that "the primary and fundamental assumption of the proposed reform is the liquidation of the Central Anti-Corruption Bureau", which is intended not only to consolidate the system of services but, above all, to rebuild trust in the institutions involved in preventing corruption.

The drafters refer to the broader international context, national security and the constitutional obligations of the Council of Ministers to ensure the legality of the activities of the special services. It draws attention to the "comprehensive deterioration of the situation in the international environment and in the immediate vicinity of the Republic of Poland", which requires strengthening the coherence of the security services' activities and eliminating institutions which, instead of strengthening national security policy, weaken it through abuse, politicisation of activities and loss of credibility.

The introduction is therefore structured on two levels: firstly, it diagnoses the dysfunction of the model in which the fight against corruption was the task of the secret services; secondly, it describes the need to reorient the fight against corruption towards institutions with greater systemic stability, more transparent supervisory mechanisms and, at the same time, an extensive investigative and analytical infrastructure, such as the Police, the Internal Security Agency (ABW) and the National Revenue Administration (KAS).

The reform is also situated within a broader international context. The justification refers to Article 6(1)(b) of the United Nations Convention against Corruption, which obliges states to establish and strengthen institutions responsible for prevention, education, and dissemination of knowledge about the risks of corruption. The authors emphasise that the modern approach to combating corruption cannot be limited to prosecuting perpetrators, but should be based on the synergy of three elements: investigative, analytical, and educational activities. Corruption is a phenomenon that "cannot be combated solely by reactive repressive measures by the state", but requires "skilful implementation of preventive measures" and "raising public awareness of the forms of corruption and ways of neutralising it".

The introduction therefore serves not only a diagnostic function, but also a normative and interpretative one. It shows that the liquidation of the CBA is part of a broader project to rebuild the rule of law, restore the depoliticisation of the services, increase the transparency of the security authorities and shift anti-corruption policy onto a more modern track in line with international standards. It recalls long-standing political and social demands for the abolition of the CBA, demands that have intensified in connection with the disclosure of numerous cases of abuse, including the use of illegal surveillance methods against political opponents and citizens who are "inconvenient for the authorities".

The overarching goal of the reform is to create an institutional model that ensures genuine apoliticality, fosters a greater culture of accountability, enhances effectiveness in identifying and combating corruption offences, and, at the same time, ensures consistency in the State's actions in the area of internal security. The introduction to the explanatory memorandum thus provides an interpretative basis for the rest of the document, presenting the liquidation of the CBA not as the elimination of an instrument in the fight against corruption, but as a necessary modernisation and restructuring of national institutions.

5.3.2. Critical diagnosis of the functioning of the Central Anti-Corruption Bureau – institutional, political, and legal conditions

The second part of the explanatory memorandum to the draft law provides an in-depth analysis of the reasons why the Central Anti-Corruption Bureau – intended by its creators to be an exceptionally effective tool for combating corruption in the public sphere – ceased to fulfil its function, both operationally and systemically. The explanatory memorandum clearly states that the CBA not only failed to perform its tasks effectively, but also became a source of problems that directly violated the standards of a democratic State governed by the rule of law, including the principles of legality, proportionality and political neutrality.

The explanatory memorandum primarily points to the growing number of cases in which the Bureau has exceeded its powers, including through the use of covert surveillance measures against individuals who were not involved in corrupt activities but in broadly understood political or civic activities. As emphasised, these activities concerned "persons inconvenient to the authorities", and the tool used included, among others, the Pegasus spyware system – a solution whose use provoked widespread public and international opposition as a violation of fundamental human rights, including the right to privacy and the confidentiality of communication. The justification emphasised that the use of such far-reaching instruments without full substantive justification and in the absence of adequate institutional control constituted a violation of the constitutional principle of proportionality.

These abuses are part of a broader systemic problem centred on the CBA's excessively broad operational powers and weak parliamentary oversight of its activities. The instruments at the disposal of the Bureau – including the possibility of using operational techniques, conducting operational surveillance, obtaining sensitive information, as well as conducting asset controls and reviewing confidential documents – created a structure which, in the justification, was described as susceptible to abuse, especially if it is detached from real anti-corruption factors and transferred to the realm of political disputes. The explanatory memorandum indicates that this is precisely what has happened: instead of being an apolitical structure that controls corruption risks in public administration, the Bureau began to "serve as a tool in the hands of those in power", leading to a "deep crisis of confidence in this institution".

In the context of the CBA's effectiveness in combating corruption, the justification relies on hard data, citing Transparency International's Corruption Perceptions Index, which shows a dramatic decline from 29th place in 2015 to 47th place in 2023, with a score of only 54 points out of a possible 100. This decline is interpreted not as the result of external political factors, but rather as an indicator of a genuine deterioration in the quality of institutional mechanisms for combating corruption. The justification emphasises that countries that are effectively strengthening their anti-corruption systems are seeing a steady increase in their scores. In contrast, Poland, despite the existence of a service with broad powers, has seen the opposite trend, which "demonstrates the ineffectiveness of the CBA as an institution responsible for combating corruption".

The critical diagnosis also covers organisational and competence aspects. The explanatory memorandum notes that the CBA undertook several activities that did not align with the logic of a special service. The Office's administrative controls and activities, such as the oversight of privatisation processes, documentation of administrative decisions, and public procurement, were particularly criticised. It was noted that many of these tasks were of a control or audit nature, i.e., closer to supervisory institutions than to specialised services, which should focus on tasks related to national security, operational work, and the detection of terrorist or international crimes. This dispersion of competences led to a "structural overload of the Bureau and blurring of its operational profile", weakening its ability to carry out truly key anti-corruption activities.

The diagnosis also includes an analysis of the CBA's cooperation with other national institutions. The justification clearly suggests that the Bureau operated in isolation, was reluctant to cooperate with the Police, the Internal Security Agency (ABW) or the National Revenue Administration (KAS), and that its organisational structure duplicated that of these services in many respects. This model not only generates inefficiency but also risks conflicts of competence and the blocking of information flows, both of which are crucial to combating systemic corruption. Instead of strengthening the security system, the CBA – through its autonomy and lack of cooperation with other institutions – began to destabilise it.

Finally, the explanatory memorandum cites an argument of a systemic nature: the existence of a special service whose main task is to combat corruption is an unusual solution compared to other EU and OECD countries. In most cases, these activities are carried out by police units, law enforcement agencies, or specialised anti-corruption agencies with an

analytical and preventive focus, rather than special services conducting operational activities. In this sense, the Polish CBA, instead of complying with international standards, was a structure that deviated from them. As emphasised in the explanatory memorandum, a modern anti-corruption system requires a combination of prevention, education, and analytical activities – elements that were of marginal importance in the CBA model, which was contrary to the recommendations of the United Nations Convention against Corruption (UNCAC).

The diagnosis contained in the justification forms a coherent narrative: the CBA was an ineffective, overly politicised, organisationally dysfunctional institution that violated civil rights and was burdened with structural design flaws that prevented it from operating effectively in a modern, democratic State. All these elements serve as an introduction to the justification for liquidating the Bureau and transferring its tasks to other institutions.

5.3.3. Systemic concept of liquidating the Central Anti-Corruption Bureau and assumptions for a new institutional architecture

After presenting a diagnosis of the CBA's shortcomings, the justification proceeds to the main part of the argument, in which the liquidation of the Bureau is presented not as an ad hoc measure, but as part of a comprehensive and well-thought-out institutional transformation. The drafters emphasise that the decision to abolish the CBA is not of a technical nature – on the contrary, it constitutes a fundamental paradigm shift, in which the State's anti-corruption policy is transferred from the area of special services to the area of specialised, systemically stable security, supervision and control bodies.

The justification clearly states that the current anti-corruption model, in which reconnaissance, control, investigation and analysis activities are concentrated in a single special service, has proved to be flawed. The liquidation of the CBA is presented as a necessary reconstruction, which allows anti-corruption tasks to be transferred to where, in the light of both Polish and international experience, they are performed more effectively, with respect for the principle of separation of powers and with less risk of political instrumentalisation.

The starting point is the assertion that the State cannot maintain a service that "betrays its statutory purpose", violates individual rights, and raises serious doubts about its political neutrality. The justification indicates that such behaviour by the CBA was not incidental, but

constituted a persistent pattern that threatened the foundations of public trust and the legitimacy of anti-corruption measures.

Therefore, the liquidation of the CBA is presented as a necessary condition for anti-corruption policy to regain:

1. social credibility
2. compliance with the constitutional legal order
3. organisational effectiveness
4. apolitical nature and resistance to abuse

The drafters clearly use the category of "institutional healing", in which the removal of an inefficient and degenerate structure becomes a necessary step before building new anti-corruption mechanisms.

A key element of the draft is the transfer of the CBA's tasks to three different bodies:

- the Police
- the Internal Security Agency
- the National Revenue Administration

It is this separation of powers that is presented as the most important philosophical change of the entire reform. According to the explanatory memorandum, the State should not consolidate investigative, preventive, and control functions in a single special service, as such a concentration of competences poses systemic risks, including the temptation to utilise operational instruments for political purposes. The liquidation of the CBA therefore leads to the dispersal of anti-corruption tasks in a way that:

- strengthens the specialisation of individual bodies
- facilitates supervision of their activities
- increases the transparency of operating mechanisms
- allows for better democratic control

The justification also emphasises that although the CBA's powers are being dispersed, the anti-corruption system is becoming more coherent thanks to the statutory introduction of coordination instruments – primarily anti-corruption safeguards.

The biggest changes concern the Police, including the establishment of the Central Anti-Corruption Bureau (CBZK). This unit is tasked with combating corruption in both operational and investigative contexts. The explanatory memorandum contains detailed arguments in favour of this solution.

Firstly, the Police have a much broader and more established organisational potential, including a developed network of local units, experience in combating economic crime and specialised departments dealing with corruption, which can be naturally integrated into the structure of the new office.

Secondly, the police operate under more transparent oversight mechanisms than the special services. They are supervised by the Minister of the Interior, not directly by the Prime Minister, and their activities are also subject to greater parliamentary and public scrutiny. Shifting the main burden of the fight against corruption to the police therefore means transferring this area of State activity from the secret services to structures subject to the transparency and oversight standards appropriate to a democratic State governed by the rule of law.

Thirdly, the Police is an institution that is more resistant to politicisation, thanks in part to its larger staff, longer tradition, and rotation mechanisms. The transfer of CBA officers to the Police is intended to preserve the Bureau's expertise while, at the same time, subjecting these staff to a more stable and controlled organisational framework. The liquidation of the CBA does not only mean the transfer of its tasks to the Police. The justification presents a detailed logic for the separation of the remaining competences.

The Internal Security Agency (ABW) is taking over tasks that are important from a national security perspective, including monitoring privatisation processes, public procurement, and the granting of concessions when they may pose systemic risks. These activities are closer to risk analysis and threat identification, which is the natural role of a special service. It was emphasised that the ABW has a much more appropriate structure and experience in conducting such analyses than the CBA, whose organisational model focused on investigative activities.

The National Revenue Administration, on the other hand, assumes tasks related to financial control and combating economic crime, which, in practice, were previously carried out by the CBA in a fragmented and inconsistent manner. The National Revenue Administration, as a body specialising in financial risk analysis and tax control, has natural competences in this area, which allows it to perform the tasks taken over from the Bureau more effectively.

The justification also includes a detailed analysis of the technical, legal, and organisational processes involved in the liquidation of CBA. The abolition of the office of the

Head of the CBA, the transfer of infrastructure, assets, operational and human resources to the Police and other authorities, and the complete phasing out of current activities were presented as sequential processes designed to ensure the smooth functioning of the anti-corruption system. According to the draft bill, the CBA liquidator is granted broad executive powers in this regard. The transfer of officers is intended to guarantee the continuation of ongoing proceedings while eliminating pathological organisational mechanisms.

The most important assumption of the third part of the explanatory memorandum is that the liquidation of the CBA will not only not weaken the anti-corruption system. Still, it is a necessary condition for this system to function efficiently and effectively. In this sense, the draft presents the liquidation of the CBA not as a "departure from anti-corruption", but as the beginning of a new phase of anti-corruption policy, in which:

- the main emphasis is on the professionalisation of institutions
- operational activities are subject to greater supervision
- prevention and risk analysis are given a statutory basis
- coordination becomes a rule of operation rather than an optional practice

In this context, the liquidation of the CBA appears not so much as the end of an era, but rather as a prerequisite for creating a new, more mature anti-corruption model that meets both legal standards and contemporary threats.

5.3.4. New mechanisms for coordinating anti-corruption activities – structure, functions, and systemic significance

The reform presented in the explanatory memorandum to the draft law not only provides for the liquidation of the Central Anti-Corruption Bureau, but also for a thorough restructuring of the organisation and management of anti-corruption activities nationwide. A key element of this change is the introduction of new coordination mechanisms into the legal system, which are to replace the current practice of a single special service operating in isolation and burdened by numerous abuses. The justification emphasised that it was precisely the lack of cooperation, organisational isolation and political exploitation of the CBA that contributed to the profound degradation of the anti-corruption system, as well as to a significant decline in Poland's international standing in rankings on transparency and the rule of law. Therefore, the new

model is based on a fundamental assumption: the State cannot fight corruption solely by relying on a single entity operating according to the logic of a special service. Still, it must create a coordinated, multi-layered system of cooperation between authorities with different competences.

The most characteristic and central element of the new system is the statutory introduction of the so-called anti-corruption shield. Until now, it has only operated in accordance with the Prime Minister's 2024 guidelines, which were not binding, depended on political decisions, and did not establish a systemic framework for permanent cooperation between services. The legislator emphasises that raising the anti-corruption shield to the level of a statute ensures its durability, transparency, and resistance to political changes. The explanatory memorandum explains that anti-corruption protection is a set of procedures obliging the Police, the Internal Security Agency, and the Military Counterintelligence Service to cooperate to increase the effectiveness of identifying and counteracting corruption, both at the stage of planning public projects and during their implementation and settlement. Its purpose is not to create a new body or institutional structure, but to provide existing services with a coordination framework that requires them to apply the procedures laid down in the Act. This framework transforms the State's model of operation from a reactive one, focused on tracking and punishing perpetrators of crimes already committed, to a preventive and analytical model based on planning, anticipating, and preventing corruption risks.

In this new system, the Prime Minister plays a central role, becoming the coordinator and chief architect of anti-corruption policy. The explanatory memorandum indicates that the Prime Minister gains the power to set priorities for action, initiate anti-corruption protection procedures for key projects, introduce binding guidelines defining the scope of cooperation between services, and assess corruption risk on the basis of analyses presented by the Police, the Internal Security Agency (ABW) and the Military Counterintelligence Service (SKW). This solution restores the logic of political accountability at the highest level, ensuring that the fight against corruption ceases to be the domain of an autonomous special service operating outside the system of ongoing control and becomes one of the components of government policy conducted within the constitutional powers of the Council of Ministers. The justification also provides for the possibility of appointing a Minister Coordinator of Special Services, who, in the event of a political decision, could take over some of the Prime Minister's duties, ensuring the continuity of coordination policy in changing political circumstances.

The new model of coordinating anti-corruption activities assumes close cooperation between the Police, the Internal Security Agency, the Military Counterintelligence Service, and, albeit to a different extent, the National Revenue Administration. The police now play a key role in anti-corruption efforts, particularly after taking over the principal investigative powers formerly exercised by the Central Anti-Corruption Bureau (CBA) following its establishment. The explanatory memorandum emphasises that the police are not only given operational and investigative tasks but also new analytical powers to identify corruption risks at an early stage. To this end, the Chief Commander of the Police is to be granted access to the operational records of the Internal Security Agency (ABW), in accordance with Article 40(2) of the Act on the ABW and the AW. This involves breaking down the existing information barrier between services and creating conditions for an integrated assessment of corruption risk, a lack of which was one of the model's main weaknesses, according to the Central Anti-Corruption Bureau (CBA).

As part of its anti-corruption measures, the ABW performs analytical and protective functions, focusing on projects that may pose a threat to national security. Its role is to identify strategic risks, in particular those related to privatisation, large public investments or concession processes. The SKW, on the other hand, operates in the defence sector, where corruption risks can have particularly serious consequences for national security. Meanwhile, the National Revenue Administration participates in the coordination system primarily by providing financial data and analyses of economic and tax risks that may be relevant for identifying corruption schemes.

The explanatory memorandum clearly emphasises that the new coordination model does not focus solely on repressive measures, but combines them with an extensive range of preventive measures. It is noted that one of the fundamental elements of modern anti-corruption systems, as recommended by the UN Convention against Corruption, is education, risk analysis, and fostering a culture of transparency in public administration. Therefore, anti-corruption protection also includes activities such as creating early warning mechanisms, developing transparency standards, introducing audit procedures, and analysing administrative processes for potential corruption vulnerabilities. The explanatory memorandum clearly emphasises that the effectiveness of anti-corruption policy depends on the balance between prevention and repression, as well as on the State's ability to identify threats before they become crimes, rather than merely punishing perpetrators after the fact.

Inter-ministerial coordination, which is at the heart of the new system, was presented as a response to the structural problems of the CBA period. Operating outside cooperation mechanisms, that service was unable to produce comprehensive analyses or respond effectively to systemic corruption because it operated in isolation from the police, special services, and tax authorities. The new model addresses this shortcoming by leveraging information sharing, common operating procedures, and data integration, encompassing operational, financial, and administrative data. This is a step towards building a State information infrastructure in which corruption risks are monitored multidimensionally, in real-time, and utilising the competences of various authorities.

The entire anti-corruption framework clearly reflects an attempt to create a system in which any public project involving a risk of corruption can be supervised by multiple services simultaneously, and the flow of information between them is guaranteed by law rather than left to the discretion of individual institution management. However, this mechanism is neither police nor operational in nature – its essence is coordination, supervision, analysis, and prevention, which means a departure from the investigative approach that dominates the CBA.

The result is a system that combines the dispersion of competences with centralised supervision. The police, the Internal Security Agency (ABW), the Military Counterintelligence Service (SKW), and the National Revenue Administration (KAS) are assigned precisely defined tasks, and the Prime Minister serves as the guarantor of consistency and uniformity of action. The whole is intended to create an institutional environment in which no entity operates in isolation, and the risk of abuse, politicisation, and arbitrariness is minimised through common procedures, transparency, and a statutory obligation to cooperate.

5.3.5. Summary

The reform involving the liquidation of the Central Anti-Corruption Bureau and the creation of new mechanisms for coordinating anti-corruption activities is one of the most comprehensive and multifaceted institutional undertakings in the history of the Polish internal security system. The explanatory memorandum to the draft law paints a picture of a profound reconstruction, the aim of which is not only to change the organisational structure, but also to completely overhaul the philosophy of combating corruption in the State.

An assessment of the CBA's functioning identified several elements that rendered this institution incapable of fulfilling its statutory mission. These problems included violations of the rule of law and democratic control principles, as well as operational abuses, including the use of illegal surveillance tools, the instrumental use of powers for political purposes, and structural isolation from other State institutions. The structure of the CBA, which combines operational, control, and analytical functions, proved in practice to be susceptible to abuse and ineffective in preventing corruption. This is confirmed by Poland's decline in international rankings, especially in the Corruption Perceptions Index, which has become an objective measure of the ineffectiveness of the existing model.

In this context, the liquidation of the CBA was not presented as a political gesture but as a logical consequence of the need to rebuild the national anti-corruption system. The justification suggests that the fight against corruption in a democratic State governed by the rule of law should be based on a balance between prevention, risk analysis, education, and targeted criminal prosecution, rather than on a centralised, broadly empowered operational body. Therefore, the tasks of the CBA have been distributed among three institutions: the Police, the Internal Security Agency (ABW) and the National Revenue Administration (KAS). Each of them is to implement those elements of anti-corruption policy that correspond to its natural competences: the Police – operational and investigative activities; the ABW – analytical and State security tasks; the KAS – financial and fiscal control.

However, the most innovative aspect of the reform is the introduction of a statutory anti-corruption protection mechanism, which serves as the foundation for the systemic coordination of State activities in this area. This protection meets international standards and complies with the recommendations of the UN Convention against Corruption, which imposes an obligation to set up specialised preventive structures. In the new model, it is not a single service with broad powers that decides on the direction of anti-corruption policy, but a network of cooperating institutions whose activities are coherently coordinated by the Prime Minister. As a result, the fight against corruption is integrated into the State management system and no longer remains in the hands of a single autonomous entity.

As a result, this reform creates a solution that combines transparency with effectiveness and political oversight with resistance to politicisation. The distribution of tasks, combined with central coordination, establishes a mechanism capable of permanently reducing the risk of corruption, identifying threats at an early stage, and enforcing accountability where

violations occur. The model based on a single, poorly controlled special service is being replaced by a multi-agent, interoperable model that complies with the standards of a democratic State governed by the rule of law.

In summary, the liquidation of the CBA and the introduction of new coordination mechanisms are not only an administrative reorganisation, but above all a restructuring of the logic of the State's anti-corruption activities. This reform aims to restore trust in public institutions, increase the transparency of decision-making processes, enhance political accountability, and ensure the effectiveness of protective, analytical, and investigative activities. It is a project that redefines the role of the State in the fight against corruption and emphasises cooperation, prevention and professionalisation – values without which the anti-corruption system cannot function effectively or legitimately.

5.4. Conclusions from the academic seminar "Comparison and Further Information on the Implementation of the PIF Directive to Fight Fraud to the Detriment of the EU"

On 24 January 2025, the Faculty of Law and Administration of Nicolaus Copernicus University in Toruń hosted a scientific seminar entitled "Comparison and Further Information on the Implementation of the PIF Directive to Fight Fraud to the Detriment of the EU", organised as part of the BETKONEXT research project.

One of the main topics of discussion was the analysis of the functioning of the Polish AFCOS and its related systemic weaknesses in protecting the European Union's financial interests. The Polish Anti-Fraud Coordination Service (AFCOS) is a key component of the European Union's national system for protecting its financial interests. Its role was shaped by Article 12a of Regulation (EU, Euratom) No 883/2013, which requires Member States to designate a body responsible for cooperation with OLAF. In Poland, this institution is located within the Ministry of Finance, with the coordinating unit entrusted to the Head of the National Revenue Administration (KAS) and the Public Funds Audit Department (DAS), which is responsible for AFCOS.

5.4.1. Structural limitations arising from the placement of AFCOS within the Ministry of Finance

The Polish AFCOS model was shaped in a manner that strongly reflects the historical conditions of government administration and previous experiences related to preparations for EU membership. Already during the pre-accession period, when Poland participated in PHARE programmes and established the first structures for protecting Community funds, the logic of assigning responsibility for combating financial fraud to the areas of audit and internal control prevailed. As a result, in 2003, the Government Plenipotentiary for Combating Financial Irregularities in the Use of European Union Funds was appointed, operating within the Ministry of Finance. According to a summary document on the origins of AFCOS, it was the Ministry of Finance, and not any investigative body or special service, that was considered the most natural place to act as a liaison between the State and OLAF, as it controlled the flow of European funds and supervised the management and control systems for EU funds.

Following the transformation of the organisational system and the establishment of the National Revenue Administration, responsibility for AFCOS's activities was formally transferred to the Head of the NRA, while the Department of Public Funds Audit provides operational institutional support. It is the DAS that "acts as the AFCOS support unit" and performs tasks related to information exchange, correspondence, cooperation with EU fund management institutions and support for OLAF's external investigations into the expenditure of EU funds under shared management. However, this is a model that, by its very nature, has built-in limitations stemming from the Department's profile and competences.

The DAS is an audit unit. Its main task is to ensure the correctness of public expenditure, conduct internal audits, assess management and control systems, and prepare analyses of the risk of irregularities. This structure does not provide for operational, investigative, or inquiry functions, which are essential parts of the modern model for protecting the Union's financial interests. As a result, the Polish AFCOS is primarily an administrative institution operating within the Ministry of Finance, focusing on document circulation, procedure analysis, and formal coordination of contacts with OLAF.

The limitations resulting from this location become particularly apparent when the scope of tasks of the Polish AFCOS is compared with the requirements of modern protection of the EU's financial interests. DAS supports OLAF's activities "in principle only in the area

of shared management", i.e., structural funds, the Common Agricultural Policy, and other programmes implemented within the Polish public administration. This means that AFCOS does not operate independently in areas where EU funds are managed directly by the European Commission, nor does it have the competence to act in relation to EU budget revenues such as customs duties, sectoral charges, or VAT-based own resources. The lack of operational tools and access to financial and operational data means that cooperation with OLAF in these areas in Poland is carried out through other institutions, with AFCOS playing only a supporting role, which weakens its position as the national coordination point.

A particular problem is AFCOS's limited access to data. DAS does not have its own analytical tools to verify financial transactions, nor does it have access to the operational records of the police, the Internal Security Agency or the Public Prosecutor's Office. This means that any actions requiring rapid fact-finding, analysis of financial flows or verification of suspected abuse must be carried out through other institutions, which have their own procedures and priorities. In practice, this means that AFCOS becomes merely a communication hub rather than a centre for analysis and coordination of operational activities. This model does not align with the concept of a "national anti-fraud service" promoted by OLAF, under which a national authority should be able to take independent initiatives, conduct its own analyses, and create a uniform picture of fraud risk at Member State level.

The location of AFCOS within the Ministry of Finance's structure also reinforces the narrow perception of protecting the EU's financial interests as a task primarily related to expenditure control. Meanwhile, financial fraud in the EU system is much broader in nature. It includes, among other things, tax fraud, VAT carousels, customs fraud, monetary and corruption offences, which affect both the Union's revenue and expenditure. From a systemic perspective, this means that the Polish AFCOS has been placed in an institutional position that covers only a fraction of the real problem, resulting in a structural asymmetry between the scope of tasks expected of OLAF and the scope of competences held by the DAS.

As a result, AFCOS does not function as a horizontal coordination centre, but rather as a segment specialising in one part of the entire system, namely EU funds under shared management. This, in turn, leads to further institutional tensions – other authorities, such as the National Revenue Administration, the police, the public prosecutor's office and the Internal Security Agency, are directly involved in activities related to the protection of the EU's

financial interests. At the same time, AFCOS remains one of many entities without the tools to coordinate activities effectively.

Given the development of European anti-fraud standards and the growing importance of mechanisms such as the EPPO, this system appears incomplete, with AFCOS's location within the Ministry of Finance determining its competences in a way that is at odds with the real needs of the state and the EU. Although formally correctly designated, the Polish AFCOS remains, in practice, an institution whose scope of activity is deliberately limited and subordinated to the logic of auditing rather than to the logic of protecting public finances comprehensively and cross-sectorally.

One of the most significant weaknesses of the Polish AFCOS is its structural dependence on other State institutions for access to data and for its ability to perform analytical, investigative, and operational activities independently. This results from both the unit's servicing of AFCOS's location in the Public Funds Audit Department and the competency model adopted by the Polish legislator, which did not equip AFCOS with the powers to independently analyse information on potential financial fraud to the detriment of the European Union.

The Public Funds Audit Department does not have access to operational registers, investigative databases, or analytical systems used by the National Revenue Administration, nor to the information resources of the Police, the Internal Security Agency, the Public Prosecutor's Office, or the Supreme Audit Office. Any request to these institutions must be made officially, through administrative channels, which significantly prolongs and complicates both national and EU information exchange. This model is based on the assumption that AFCOS is not an investigative body but a coordinating one, and therefore obtains all information from other entities – none of which, however, have a statutory obligation to give priority to its requests, nor is any of them responsible for building a uniform picture of fraud risk in Poland.

As a result, the Polish AFCOS operates reactively rather than proactively. It lacks the tools to independently monitor financial transactions, analyse dispersed data, or assess threats to the EU's financial interests on an ongoing basis. In practice, each stage of its work depends on whether other institutions provide it with the relevant data, in what form they do so, and how quickly they respond to its requests. As these institutions are guided by their own priorities

and burdened with other statutory tasks, the exchange of information with AFCOS is often not treated as a high priority.

This dependence on other institutions also has a qualitative dimension. As AFCOS has no operational or investigative powers, it cannot independently assess the reliability of the data it receives. Its role is therefore limited to transmitting information between national institutions and OLAF, without the possibility of critically analysing or synthesising the evidence in a manner that meets EU standards. This means that the Polish model for protecting the EU's financial interests lacks a central body to direct national anti-fraud activities. Each unit remains responsible for its own part of the system, and AFCOS is unable to provide operational impetus or initiate additional analyses.

In Poland, AFCOS therefore primarily functions as a correspondence and reporting institution, operating without its own operational tools and without influencing the pace, scope, or quality of the activities of other entities involved in protecting the EU's financial interests.

5.4.2. The liability of collective entities in the protection of the European Union's financial interests

The second key element of the discussion concerned the liability of collective entities in protecting the financial interests of the European Union. It was pointed out that collective entities – in particular, local government units, commercial law companies, non-governmental organisations, and other institutions implementing EU projects – are the main administrators of EU funds, which makes them a central link in potential abuses. The analysis revealed that irregularities related to EU funds are generally structural rather than individual in nature, as exemplified by bid rigging, fictitious documents, cost manipulation, and hidden conflicts of interest in co-financed projects.

The discussion focused on the origins of collective liability in various European countries, including Belgium, France, and Poland. It highlighted the ongoing dogmatic problem of attributing an act to a legal fiction, namely a legal person. Attention was drawn to limitations, such as the exclusion of State or local government liability, which further weakens the system's effectiveness. The discussion also focused on the requirements of the PIF

Directive, which requires Member States to introduce effective and dissuasive mechanisms for holding legal persons liable for offences against the financial interests of the EU.

It was emphasised that, despite theoretical and practical difficulties, the liability of collective entities plays an important role as a complement to individual liability – it enables the recovery of illegally obtained benefits, strengthens deterrence, and has an important symbolic dimension, highlighting the importance of sound management of public funds. The conclusions emphasised that although Polish regulation in its current form is imperfect, it has significant development potential and can be an important tool for strengthening the protection of the European Union's financial interests.

References

- Aldovrandi, P. (2019). La nozione di "fatture o altri documenti per operazioni inesistenti": la Suprema Corte conferma la rilevanza della falsità materiale e approfondisce la frattura tra "legge" e "diritto vivente", nota a Cass. pen., sez. III, 25 ottobre 2018, n. 6360, Indice penale, 281 ff.
- Amarelli, G. (2018). Indebita percezione di erogazioni a danno dello Stato, in Amarelli-Fiore (eds.), I delitti dei Pubblici Ufficiali contro la Pubblica Amministrazione, Giappichelli, 79 ff.
- Ambrosetti, E.M. (2022). I reati tributari, in Ambrosetti, Mezzetti, Ronco (eds.), Diritto penale dell'impresa, Zanichelli, 417 ff.
- Ardizzone, G. (2024). Le frodi a danno dei Fondi Agricoli Europei tra ne bis in idem e proporzionalità, Archivio penale, 1 ff.
- Ardizzone, G. (2025). Il nuovo assetto del diritto penale tributario: un'analisi del d.lgs. 14 giugno 2024, n. 87, Legislazione penale, 1 ff.
- Basile, E. (2020). Il recepimento della direttiva PIF in Italia e l'evergreen art. 316-ter, Diritto penale contemporaneo – Rivista trimestrale, 178 ff.
- Bellacosa, M. (2016). La riforma dei reati tributari nella prospettiva europea, in Del Vecchio, A., Severino, P. (eds.), Tutela degli investimenti tra integrazione dei mercati e concorrenza di ordinamenti, Cacucci, 279 ff.
- Bellacosa, M. (2020). I reati tributari e i reati di contrabbando, in Lattanzi, G., Severino, P. (eds.), Responsabilità da reato degli enti. Vol. I, Diritto sostanziale, Giappichelli, 611 ff.
- Bellacosa, M., De Bellis, M. (2023). The protection of the EU financial interests between administrative and criminal tools: OLAF and EPPO, Common Market Law Review, Vol. 60 (1), 15 ff.
- Birritteri, E., Tatì, E. (2022). Cooperative Compliance Measures to Prevent Organised Crime Infiltrations and the Protection of EU's Financial interests. A New Gold Standard in the Implementation of the Italian Recovery and Resilience Plan? in Diritto penale contemporaneo, n. 3, 2240-7618

- Bisori, L. (2021). sub art. 640-bis, in Dolcini-Gatta (eds.), Codice penale commentato, Tomo III, Giuffrè, 7284 ff.
- Cáceres Casado, M. (2024). "Fraude carrusel y responsabilidad penal de las personas jurídicas: a propósito de la Sentencia de la Audiencia Nacional n. 5/2021, de 3 de marzo", La ley penal: revista de derecho penal, procesal y penitenciario, No. 167
- Capdeferro, O. (2025). El sistema de compliment normatiu amb protección efectiva de persones alertadores. IEA, Barcelona
- Carbajo Domingo, M.Á. (2023). La posible inconstitucionalidad de la Ley 2/2023: la creación de espacios de impunidad ajenos al contencioso-administrativo. El descontrol de la actividad administrativa de los artículos 13 a 20 de la Ley 2/2023", El consultor de los Ayuntamientos, 143 ff.
- Careel, S. & De Smedt, J. (2022), Diversion, Restorative Justice and Mediation in PIF Crimes: National Report, Belgium, Brussels: DRAMP
- Carmignani, S., Papini, G. (2022). Le frodi in agricoltura, Diritto agroalimentare, 203 ff.
- Covolo, V. (2011). The legal framework of OLAF investigations. What lessons for the European criminal area?, NJECL, Vol. 2 (2), 201 ff.
- D'Arcangelo, F. (2017). L'emissione di fatture per operazioni inesistenti ed i limiti al concorso di persone nel reato tra emittente ed utilizzatore, in Bricchetti, Veneziani (eds.), I reati tributari, in Palazzo, Paliero (eds.), Trattato teorico-pratico di diritto penale, Giappichelli, 271 ff.
- De Bellis, M. (2021). Multi-level administration, inspections and fundamental rights: Is judicial protection full and effective?, GLJ, Vol. 22, 171 ff.
- Del Gatto, S. (2024). La dimensione amministrativa del conflitto di interessi e il principio di buona amministrazione, Rivista trimestrale di diritto pubblico, No. 2, 311 ff.
- Dianese, G., Grozdev, D. (2022). Criminal and Administrative Procedures in Protecting the Financial Interests of the EU, Eucrim, Vol. 17(4), 279 ff.
- Donini, V.M. (2024). La simbiosi tra accountability e whistleblowing nel quadro del governo aperto: un'analisi delle dinamiche e delle interazioni, federalismi.it, No. 16, 221 ff.

- Falsitta, V., Faggioli, M. (2017). La normativa tributaria di riferimento e le definizioni legali, in Bricchetti, Veneziani (eds.), I reati tributari, in Palazzo, Paliero (eds.), Trattato teorico-pratico di diritto penale, Giappichelli, 18 ff.
- Gullo, A. (2000). Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640-bis c.p.), in Marini, Paterniti (eds.), Dizionario dei reati contro l'economia, 528 ff.
- Inghelram, J.F.H. (2011). Legal and Institutional Aspects of the European Anti-Fraud Office (OLAF). An Analysis with a Look Forward to a European Public Prosecutor's Office, Europa Law Publishing, 189.
- Ingrassia, A. (2020). Il bastone (di cartapesta) e la carota (avvelenata): iniezioni di irrazionalità nel sistema penale tributario, Diritto penale e processo, 307 ff.
- Ingrassia, A. (2024). Tra il dire e il fare: le modifiche del c.d. decreto sanzioni ai reati di omesso versamento e di indebita compensazione, Diritto penale e processo, 1568 ff.
- Jurić, M. (2022). The Players in the Protection of the EU's Financial Interests, Eucrim, Vol. 17(3), 214 ff.
- Kratsas, G. (2012). A case for OLAF: The place and role of the Anti-Fraud Office in the European Union context, EPL, Vol. 18 (1), 65 ff.
- Lanzi, A., Aldovrandi, P. (2020). Diritto penale tributario, Cedam
- Ligeti, K., Robinson, G. (2017). Transversal report on judicial protection, in Luchtman M., Vervaele, J., Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement authorities (ECN/ESMA/ECB), Utrecht University, 219 ff.
- Manacorda, S. (2001). Corruzione internazionale e tutela penale degli interessi comunitari, Diritto penale e processo, 415 ff.
- Martines, F. (2022). Azione amministrativa e conflitto di interessi. In: Scritti in onore di Maria Immordino. vol. III, Naples, Editoriale Scientifica, 2227 ff.
- Martini, A. (2010). Reati in materia di finanze e tributi, in Grosso, Pagliaro, Padovani (eds.), Trattato di diritto penale, Giuffrè
- Mattarella, B.G. (2013), La prevenzione della corruzione in Italia. Commento a l. 6 novembre 2012, n. 190, Giornale di diritto amministrativo, No. 2, 123 ff.

- Mazzanti E. (2020), Le frodi agricole nello specchio della tutela penale degli interessi finanziari UE, Rivista di diritto agroalimentare, 106 ff.
- Mezzetti, E. (2010). voce Frodi comunitarie, Digesto discipline penalistiche, Utet, 313 ff.
- Musco, E., Ardito, F. (2021). Diritto penale tributario, Zanichelli
- Nato, A., Ramotti, C., Sabia, R., Tatì, E. (eds.) (2025). EU integration through the lens of financial interests: a comparative analysis from an Administrative and CriminalLaw perspective, BETKONEXT working paper, passim.
- Nato, A., Sabia, R., E. Tatì, E. (eds.) (2024). The Institutional 'Constellation' for the Protection of the EU's Financial Interests. Past, Present and Future", BETKONEXT workingpaper, passim.
- Parajó Calvo, M. (2023). El sistema interno de información sobre infracciones normativas en las entidades locales, in Galán Galán, Alfredo & Mahillo García, Petra (dirs.), Canales de información y protección del denunciante en las Administraciones locales: estudios sobre la Ley 2/2023, de 20 de febrero. Fundación Democracia y Gobierno Local, Madrid, 53 ff.
- Pelissero, M. (1991). Truffa aggravata per il conseguimento di erogazioni pubbliche, Rivista italiana di diritto e procedura penale, 923 ff.
- Pelissero, M. (2001). Commento alla l. 29 settembre 2000, n. 300, Legislazione penale, 991 ff.
- Pérez Monguió, J. M. (2023). La protección del informante como piedra angular del sistema del whistleblowers, in Pérez Monguió, J. M. & Fernandez Ramos, S., El nuevo sistema de protección del informante, Bosch. Madrid, 227 ff.
- Perini, A. (2008). Diritto penale tributario, in Cianci, Perini, Santoriello (eds.), La disciplina penale dell'economia, T. II, Utet
- Picciotti, V. (2022), L'Italia "ritocca" le norme PIF (e non solo), Sistema penale, 8th November 2022
- Picotti, L. (2006). L'attuazione in Italia degli strumenti dell'Unione Europea per la protezione penale degli interessi finanziari comunitari, Rivista trimestrale di diritto penale dell'economia, 615 ff.
- Ponce Solé, J. (2025). La condición de interesado del informante y su derecho y legitimación para recurrir las decisiones de no tramitar las Comunicaciones,

in Sierra Rodríguez, J. (dir.), Sistemas de información y protección de informantes en España. Aranzadi: Madrid (2025), 107 ff.

- Romano, M. (2002). Abusi di finanziamenti comunitari ed indebita percezione di erogazioni a danno dello Stato, Diritto penale e processo, 269 ff.
- Romano, M. (2013). sub art. 316-ter c.p., I delitti contro la Pubblica Amministrazione. I delitti dei pubblici ufficiali, Giuffrè, 82 ff.
- Rubechini, P. (2024), Della delazione virtuosa. La segnalazione di illecito quale strumento di protezione dell'interesse generale, Rivista trimestrale di diritto pubblico, No. 2, 409 ff.
- Ruta, G. (2017). La dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, in Bricchetti, Veneziani (eds.), I reati tributari, in Palazzo, Paliero (eds.), Trattato teorico-pratico di diritto penale, Giappichelli, 183 ff.
- Seminara, S. (2017). sub Art. 316-ter, in Forti, Seminara, Zuccalà (eds.), Commentario breve al codice penale, Cedam, 1026 ff.
- Soana, G. (2023). I reati tributari, Giuffrè
- Subirana de la Cruz, S. & López Donaire, M. B. (2023). Compliance público, in Fortuny Cendra, M. (dir.). 250 preguntas y respuestas sobre la Ley de Protección de los Informantes. Aranzadi: Cizur Menor, 147 ff.
- Tripodi, A.F. (2022). *Ne bis in idem* europeo e doppi binari punitivi, Giappichelli
- Weyembergh, A., Brière, C. (2018). The future cooperation between OLAF and the European Public Prosecutor's Office, NJECL, Vol. 9 (1), 62 ff.

Documents

- European Commission (2018). The concept of Tax Gaps. Report III: MTIC Fraud Gap Estimation Methodologies. FISCALIS 2020 Tax Gap Project Group, subgroup VAT fraud (FPG/041).

- ANAC (2023). Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne.
- Council of State (Spain). Opinion 1361/2022, of 8 September 2022
- European Commission (2024). Report from the Commission to the European Parliament and the Council on the implementation and application of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law
- European Commission. Measures adopted by the Member States to protect the EU's financial interests -Implementation of article 325 TFUE, SWD(2025) 228 final. 25 July 2025
- European Public Prosecutor's Office (2023). Belgium: EPPO dismantles customs fraud ring operating at Liège Airport – €310 million in estimated damages. EPPO. Retrieved 16 November 2025, https://www.eppo.europa.eu/en/media/news/belgium-eppo-dismantles-customs-fraud-ring-operating-liege-airport-eu310-million
- European Public Prosecutor's Office (2024). Seven arrested in probe of €13 million VAT fraud in Belgium and the Netherlands. EPPO. Retrieved 15 November 2025, https://www.eppo.europa.eu/en/media/news/seven-arrested-probe-eu13-million-vat-fraud-belgium-and-netherlands
- Federal Institute for Human Rights (FIRM–IFDH) (2025). Guide for Whistleblowers
- Federal Ombudsman (2024). Annual report 2024. Federal Ombudsman of Belgium
- Presidenza del Consiglio dei ministri, Dipartimento per gli Affari Europei, Nucleo della Guardia di Finanza per la repressione delle frodi nei confronti dell'Unione Europea (2024). Misure di prevenzione e contrasto alle frodi e agli altri illeciti in danno del P.N.R.R., 60 ff.
- Directorate-General for Taxation and Customs Union (European Commission) (2024). "VAT compliance gap due to Missing Trader Intra-Community (MTIC) fraud" final report

- Presidenza del Consiglio dei ministri, Dipartimento per gli Affari Europei, Comitato per la lotta contro le frodi nei confronti dell'Unione europea (2023). Relazione annuale, 63 ff.
- Protocollo d'intesa relativo ai rapporti di collaborazione tra la Guardia di Finanza e Cassa Depositi e Prestiti S.p.A., aprile 2025: https://www.gdf.gov.it/it/amministrazione-trasparente/provvedimenti/provvedimenti-dirigenti/accordi-stipulati-dallamministrazione/protocollo-d2019intesa-con-la-cassa-depositi-e-prestiti-s-p-a/protocollo-dintesa/@@download/file_principale
- Protocollo d'intesa tra Il Dipartimento della Ragioneria Generale dello Stato del Ministero dell'Economia e delle Finanze e il Comando Generale della Guardia di Finanza, dicembre 2021: https://www.mur.gov.it/sites/default/files/2024-06/PNRR_Str_ATT_Protocollo%20di%20intesa%20GdF%20e%20RGS%20-%20MEF.pdf
- RTBF (2024). Le centre équestre des Lacs de l'Eau d'Heure dans le collimateur de l'Europe. Retrieved 16 November 2025, https://www.rtbf.be/article/le-centre-equestre-des-lacs-de-l-eau-d-heure-dans-le-collimateur-de-l-europe-11465805
- Spanish Government. National Plan to Combat Corruption. 9 July 2025
- Vlaamse Regering (n.d.). Structuur van België en bevoegdheidsverdeling. Vlaanderen.be. Retrieved 16 November 2025, https://www.vlaanderen.be/vlaanderen-intern-communicatie/internationale-communicatie-over-vlaanderen/structuur-van-belgie-en-bevoegdheidsverdeling