EU CYBER VAT

Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study

Policy Recommendations

Andrea Di Nicola, Roberto Flor, Gabriele Baratto, Denise Boriero, Giulia Perrone
Centre for Security and Crime Sciences (CSSC)
University of Trento and University of Verona (Italy)

Co-funded by
the European Union

EU CYBER VAT - Policy Recommendations

Authors:

Andrea Di Nicola

Roberto Flor

Gabriele Baratto

Denise Boriero

Giulia Perrone

The ***research team*** *included (in alphabetical order):* Gabriele Baratto, Denise Boriero, Silvia Civitella, Andrea Di Nicola, Roberto Flor, Elena Ioriatti, Beatrice Panattoni, Giulia Perrone, Beatrice Rigon, Ludovica Tomasini

----

Project: EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study

Deliverable 3.1

Beneficiary

CSSC Centro di Scienze della Sicurezza e della Criminalità

UNIVERSITÀ DI TRENTO

UNIVERSITÀ di VERONA

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Anti-Fraud Office (OLAF). Neither the European Union nor the granting authority can be held responsible for them.

Centre for Security and Crime Sciences (CSSC) of the University of Trento and the University of Verona

www.cssc.unitn.it

Trento, July 2025

Table of contents

1. Introduction

Value-Added Tax (VAT) remains one of the most significant sources of public revenue both at EU and national level. However, the digitalization of commerce and the growing sophistication of cybercriminals have led to a sharp increase in cyber VAT fraud, posing an escalating threat to tax integrity, state revenues, and fair market competition.

For the purposes of the EU Cyber VAT project and this policy recommendations:

> *Cyber VAT fraud involves the use of technology to facilitate the criminal activity as a whole or to assist in one or more of its stages/phases. The use of technology at one or more stages/phases may include the creation of shell companies using forged documents or identities, the conduct of online transactions and the sale of online goods, including digital goods.*

In other words, Cyber VAT fraud refers to both a cyber enabled and a cyber assisted crime that consists of VAT fraud facilitated by new technologies. Such facilitation can take place: a) at various stages (e.g. the financial transaction stage, where the ability to conceal cash flows can be facilitated); b) through certain activities (e.g. the creation of false documents or the establishment of fake companies); c) through the creation of new intangible goods generated by technology / digital goods (e.g. software, carbon credits).

The legal and criminological analyses conducted in the earlier phases of this project—on which these policy recommendations are based—have identified both the defining characteristics of the phenomenon and the relevant legislative frameworks at the European level and within individual Member States. Through a comprehensive review of existing literature, analysis of current legislation, and consultations with national experts and stakeholders, several critical challenges, as well as notable strengths, have emerged. If these findings are effectively addressed and shared among relevant actors, they could play a significant role in mitigating the phenomenon.

Building on the study's key findings, which are discussed in detail below, a set of policy recommendations is proposed at both the EU and national levels.

Project **EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study.**

General objective

The **general objective of EU CYBER VAT project** is to assess the adequacy of the current legal framework at EU and Member State level with regard to combating cyber-VAT fraud and to propose solutions to make it more effective and efficient at EU and Member State level. Using the method of comparative law research, the project will investigate whether the European criminal law framework for VAT fraud under the PIF Directive, its implementation by Member States, and national criminal law provisions can provide a sufficient level of legal protection against the intersection of VAT fraud and cybercrime. As these are cross-border and particularly serious crimes, the degree of harmonisation between national rules must always be monitored and ensured.

Specific objectives

The general objective of the project can be divided into the following 3 specific objectives (SO):

- To provide an analysis of cyber-VAT frauds in the European Union from an empirical criminological point of view, with special attention to the modus operandi as well as the characteristics of the actors involved. The new threats related to the digitalization of tax transactions will be assessed from a criminological perspective, in order to provide a basis for evaluating the adequacy of measures against cyber-VAT fraud in the EU and activities to detect and investigate cyber-VAT fraud by tax and law enforcement authorities;
- To provide an account of the transposition of EU criminal law into national legislations to specifically prevent and combat cyber-VAT fraud and an account of the differences between the relevant national legislations of the Member States as well as national best practices;
- To elaborate, from the dual perspective of substantive criminal law and criminal procedure, recommendations and proposals to improve the EU regulation and the national anti-fraud strategies (NAFS) against cyber-VAT fraud in order to address the new threats to the financial interests of the European Union in the context of the digital age. This will take particular account of MTIC in the digital marketplace, exploring the possibility of introducing forms of service provider accountability to prevent cyber-VAT fraud. It will also promote a higher level of harmonisation in the regulation of cross-border cyber-VAT fraud, especially when it occurs in the context of e-commerce activity.

Funding

Co-funded by the European Union – European Commission, Directorate-General for European Anti-Fraud Office (OLAF) – Union Anti-Fraud Programme – EUAF.

2. Substantive criminal law

2.1 Harmonisation, legal convergence and integration in the EU

Both from the analysis of the literature on the subject (Foffani et al., 2019; Farkas et al., 2019; European Commission – OLAF Bernardi&Negri, 2015) and from what emerged from the first online focus group conducted together with the selected national experts reveal the cross-border nature of cyber VAT fraud and the need for stronger EU-level coordination.

The **PIF Directive** (Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law) remains essential for defining and prosecuting offences that harm the EU budget. By setting a baseline for the criminalisation of fraudulent conduct and associated sanctions, it aims to foster coherence among national systems and enhance cross-border cooperation. Its importance is heightened by the growing complexity of fraud schemes and the scale of EU funding distributed through mechanisms such as the Recovery and Resilience Facility. Ensuring that the Directive is fully and effectively implemented is thus critical to upholding the rule of law, ensuring financial accountability, and reinforcing mutual trust among Member States.

The Directive already provides for, and indeed anticipates, a process of harmonisation among Member States' criminal law frameworks. However, as demonstrated in the preceding legal analysis, while there is a generally high level of formal compliance—particularly with key provisions such as **Article 3** (concerning VAT fraud committed by natural persons), **Article 7** (sanctions on natural persons), **Article 6** (liability of legal persons), and **Article 9** (sanctions on legal persons)—the harmonisation process remains incomplete.

In addition, the Directive establishes only **minimum standards**, leaving significant room for variation in implementation, interpretation, and enforcement at the national level. This divergence risks undermining the effectiveness of the EU's collective efforts to protect its financial interests and ensure the consistent application of criminal law across the Union.

There are also divergences concerning the subjective element of the offence: in some Member States, criminal liability is established for both intentional and negligent conduct. Several experts have highlighted the need for a **harmonised approach to criminal liability** that extends beyond intentional misconduct to include cases of negligence where appropriate. This would ensure a broader scope of accountability for actions that harm the financial interests of the European Union.

Moreover, **Member States should be strongly encouraged to explicitly incorporate aggravating circumstances** for VAT fraud committed by organised criminal groups, in full alignment with Article 8 of the PIF Directive, rather than relying solely on general aggravating provisions applicable to all offences. Indeed, **large-scale cross-border VAT fraud schemes are often orchestrated by organised criminal networks**, which operate not only to generate illicit profits but also to launder the proceeds of other criminal activities.

In view of the above, the policy recommendations to strengthen harmonisation, legal convergence and integration in the EU are as follows:

1. <u>Strengthen enforcement and monitoring of the PIF Directive</u>

   To promote uniform and effective implementation across the EU, the **European Commission** should strengthen its monitoring, evaluative, and support mechanisms—particularly in Member States where compliance is partial, ambiguous, or not fully aligned with the Directive's intent. This may involve a multi-faceted approach that includes the provision of targeted **legal and**

technical assistance, tailored to the specific legislative and institutional challenges faced by individual Member States.

2. Promote further harmonisation of the subjective element of the VAT-related offences

   Entourage MSs to adopt a more harmonised approach to criminal liability, including **negligent conduct** where justified, in line with expert recommendations and the evolving complexity of fraud schemes.

3. Ensure pacific aggravating circumstances for organised VAT fraud

   As foreseen in **Article 8 of he PIF Directive**, rather than relying solely on general provisions.

4. Institutionalise per-learning and knowledge-sharing platforms

   The **European Commission** could expand and formalise **peer-learning platforms** more broadly as a strategic tool to support the implementation of EU legal instruments, particularly in areas requiring close coordination between national legal systems and EU law. Such platforms would enable national authorities to exchange best practices, clarify interpretative challenges, and work towards greater convergence in the practical application of EU legislation.

5. Broaden and systematise stakeholder engagement

   Within the context of EU cyber VAT project, the exchange of knowledge and perspectives among national experts and stakeholders proved to be both **valuable and insightful**, contributing meaningfully to mutual understanding. However, these exchanges were **limited in scope and scale**, underscoring the need for more systematic, structured, and inclusive mechanisms of engagement. It is therefore essential that future initiatives ensure the **broad and sustained involvement of diverse stakeholders.** Bringing together these varied perspectives can foster a more comprehensive understanding of the challenges faced by Member States in implementing EU law and can help identify practical solutions grounded in real-world experience.

   Institutionalising such dialogue beyond ad hoc consultations or project-based activities, the EU could enhance **mutual trust, legal coherence, and administrative capacity** across Member States. In doing so, peer-learning platforms would not only serve the transposition and enforcement of specific directives like the PIF Directive, but also contribute to the **overall strengthening of the EU's legal and governance architecture**, particularly in areas involving complex cross-border cooperation and shared competences, as it is the protection of the European Union's financial interests.

2.2 Regulatory reforms

A critical discussion on the need for regulatory reform emerged from both the analysis of relevant literature (Farkas et al., 2019; Lasagni, 2015; Llopis-Gilabert et al., 2022) and the insights gained during the first online focus group with selected national experts, particularly concerning the potential introduction of a new offence specifically addressing cyber VAT fraud.

The majority of Member States consider cyber VAT fraud to fall under the traditional category of VAT fraud, owing to the inherently adaptable and free-form nature of the offence. The prevailing consensus among national experts is that **introducing a distinct criminal offence specifically for cyber VAT fraud is unnecessary, highlighting the need for regulatory reform that extends beyond the mere creation of new criminal categories**. Cyber VAT fraud is largely regarded as a technological evolution of traditional VAT fraud, which can be effectively addressed within the existing legal frameworks. However, some experts suggest that it may be appropriate to introduce an **aggravating circumstance for VAT fraud cases involving**

the use of cyber elements, in order to reflect the increased complexity and potential impact of such offences.

There is a shared understanding that the creation of new criminal offences or the classification of cyber elements as aggravating circumstances may, in any event, be less effective than investing in the strengthening of investigative and technical capacities. In particular, the development of **real-time monitoring tools, advanced data analytics (including those powered by artificial intelligence), and interoperable systems capable of supporting efficient cross-border enforcement is considered a more pragmatic and impactful approach.** These dimensions—specifically relating to cross-border cooperation and the use of technological tools in criminal investigations—will be examined in greater detail in the following sections, as they represent key recommendations that emerged throughout the course of this project.

From a structural legal perspective, it is also important to recognise that in many Member States, VAT fraud is not codified as a distinct criminal offence but is instead subsumed under broader categories such as general fraud or tax evasion. As a result, introducing a specific offence for cyber VAT fraud would not only be unnecessary but also incompatible with certain national legal systems. **Rather than creating a cyber-specific offence, the priority should be to establish a clear, harmonised definition of VAT fraud at the EU level.** Such harmonisation would enhance legal clarity, improve judicial cooperation, and support more consistent enforcement practices across Member States.

Discussions among national experts also revealed a strong consensus that **administrative liability for legal persons is often more effective than criminal liability in addressing VAT fraud.** Administrative frameworks are generally better equipped to promote corporate compliance, deliver proportional and timely sanctions, and mitigate the risks associated with over-criminalization. Consequently, to enhance the efficiency and proportionality of enforcement in VAT fraud cases, **Member States should be encouraged to strengthen their administrative liability regimes for legal persons, ensuring these are robust, dissuasive, and consistently enforced.** Such an approach can increase compliance levels while alleviating pressure on national criminal justice systems.

According to some stakeholders, a further regulatory reform in the area of fiscal policy could involve the implementation of a **generalized split payment regime, particularly targeted at sectors traditionally characterized by a higher incidence of VAT fraud.**

In light of the above, the policy recommendations aimed at regulatory reforms, are as follows:

1. Do not introduce a separate offence for cyber VAT fraud

   Maintain cyber VAT raid within the broader category of VAT fraud, recognising its nature as technological evolution of existing criminal behaviours. Avoid fragmentation and potential conflict with national legal systems where VAT fraud is not codified as separate offence

2. Harmonise the definition of VAT fraud at the EU level

   Work toward establishing a **uniform, EU-level definition of VAT fraud to enhance legal clarity, judicial cooperation and consistent enforcement** across MSs

3. Consider cyber elements as aggravating circumstances

   Encourage Ms to include **explicit aggravating circumstances for VAT fraud committed using cyber tools or digital platforms**, to reflect increased sophistication and impact

4. Prioritise investment in investigative and technological capacities

   Promote the development and employment of **real-time monitoring tools, Ai powered data analytics, interoperable systems that facilitate cross-boarder cooperation** in criminal investigations

5. Strengthen administrative liability regimes for legal persons

Reinforce administrative liability frameworks that and robust, dissuasive and consistently applied; leverage administrative mechanisms to **increase corporate compliance** and reduce the burden on criminal justice systems

6. Explore fiscal policy measures such as sector-specific plot payment regimes

Assess the potential of introducing **generalised or sectors-specific split payment regimes**, as part of a preventive regulatory strategy

3. Criminal procedure and investigations

3.1 Specialised and more efficient investigations

As previously noted, the introduction of a new category of criminal offence for cyber VAT fraud does not appear necessary. Rather, the primary challenge in this domain—consistent with broader trends in cybercrime—concerns the investigative phase. The detection and collection of evidence are significantly complicated by the inherently immaterial, digital, and often transnational nature of such offences. This complexity suggests that establishing new offences or classifying cyber elements as aggravating circumstances would be less effective than investing in the enhancement of investigative and technical capabilities.

A broad consensus among experts supports the view that the creation of specialised investigative units, the upgrading of technical resources, and the deployment of advanced digital tools represent more practical and impactful strategies for addressing cyber-enabled VAT fraud. Even in instances where digital components are integral to the commission of the offence, as is characteristic of cybercrime in its broader sense, priority should be given to improving the regulation of investigative procedures—particularly those related to the collection, processing, and analysis of electronic evidence. There is a clear and growing need for real-time monitoring tools, sophisticated data analytics (including AI-driven technologies), and interoperable systems capable of supporting effective cross-border cooperation and enforcement.

According to stakeholders and the national experts, to enhance the effectiveness and coherence of VAT and cyber VAT fraud enforcement across the European Union, a set of institutional, legal, and procedural reforms should be prioritised. Two overarching areas emerged as particularly significant from the comparative analysis of Member States' responses and expert discussions, specialised training, institutional capacity building and legal harmonisation and procedural reform.

In order to assure specialised and ore efficient investigations:

1. Invest on specialised training and specialise investigative unit

   Many Member States stressed the urgent need for **comprehensive training programmes** and structural reforms aimed at equipping investigators, prosecutors, and judges with specialised knowledge in economic crime and cyber fraud; develop **minimum standards for institutional capacity,** including trained personnel in cyber investigation, economic crime analysis, and digital evidence handling. Notably, not all Member States currently possess specialised law enforcement bodies dedicated to economic and fiscal crime, which in some cases creates significant obstacles to the effective investigation and prosecution of VAT fraud. Strengthening institutional capacity through dedicated units is therefore essential to ensure more consistent and efficient enforcement across the EU.

2. Promote EU-wide specialised training and curricula

   Development of national and EU-wide curricula, support for cross-border secondments and exchanges, and the establishment of dedicated fiscal crime units with interdisciplinary expertise in law, finance, and digital technologies. Propose the creation of an EU Training Centre for Financial and Cyber Crime, possibly under the aegis of CEPOL or Eurojust, to coordinate **standardised curricula, cross-border secondments, and knowledge exchange.**

3. Enhance procedural harmonisation

Revise existing EU instruments (e.g., the European Investigation Order, the PIF Directive) to include **minimum procedural guarantees**, shared evidentiary thresholds, and access to digital investigative tools, particularly in terms of available tools, evidentiary standards, and investigative powers. Once more, the lack of coherence across Member States hampers the effectiveness of cross-border investigations and creates disparities in enforcement.

4. Encourage the establishment of specialised judicial tracks

Provide EU funding and best-practice guidelines for the establishment and operation of financial crime chambers within national judicial systems.

5. Align statutes of limitations with complexity of transnational crime

Implement minimum limitation periods consistent with Article 12 of the PIF Directive, ensuring sufficient timeframes for investigations to unfold.

6. Align statutes of limitations with complexity of transnational crime

Implement minimum limitation periods consistent with Article 12 of the PIF Directive, ensuring sufficient timeframes for investigations to unfold.

3.2 Use of technology in prevention and investigations

Law enforcement authorities across the European Union employ a diverse array of investigative tools to combat VAT fraud, adapting these instruments to national legal frameworks while converging around common European standards. National experts consistently report that investigative practices—such as data analytics, risk-based audits, search and seizure operations, and inter-agency cooperation—remain foundational in addressing both traditional and cyber-enabled forms of VAT fraud. Though not originally designed for cybercrime, these tools are increasingly adapted to address the evolving digital nature of VAT fraud.

A broad consensus among Member States and experts suggests that the emergence of cyber VAT fraud does not necessitate entirely new investigative categories. Rather, the primary challenge lies in modernising and strengthening existing mechanisms to make them fit for purpose in the digital age. This includes enhanced forensic capacities to gather and process digital evidence, expanded use of automated screening tools such as VIES, and the application of advanced surveillance techniques and witness interviews in technologically complex cases.

Cross-border cooperation remains a cornerstone of effective investigation due to the transnational character of VAT fraud schemes. Joint task forces, intelligence-sharing platforms, and harmonised procedures play a key role in overcoming jurisdictional and legal obstacles. However, various national experts and stakeholders, and the academic literature (Merkx & Verbaan, 2019; OECD, 2017;) underscore the need for deeper technological integration, improved investigative coordination, and legal innovation.

Furthermore, ICT policies across the EU remain fragmented. While all Member States maintain ICT crime strategies, relatively few explicitly address VAT fraud—and fewer still focus on cyber VAT fraud. There is widespread recognition of the need to better harness technological infrastructure and to develop cohesive policy frameworks that respond to the specificities of cyber-enabled tax offences.

Among the key recommendations are:

1. Technological modernisation of investigative tools
   - Invest in AI-based anomaly detection, real-time transaction monitoring, and digital forensics tools—including lawful hacking—for complex VAT fraud investigations.

- Facilitate the integration of **risk-based and automated audit systems to proactively detect suspicious behaviour.**

2. Interconnection of National data systems

    - Promote the development of **interoperable databases across Member States** to enable seamless data cross-checks.
    - Establish secure channels for real-time data exchange between tax administrations and law enforcement bodies.

3. Harmonisation of digital infrastructures

    - Create **EU-wide digital platforms for investigative coordination**, reducing inefficiencies caused by nationally fragmented ICT systems.Develop common technical standards and legal protocols for digital evidence handling and cyber-enabled investigations.

4. Specialised Training and Dedicated Units

    - Encourage Member States to establish fiscal crime units with cross-disciplinary expertise in law, finance, and digital technology.
    - Support the development of **EU-level training curricula** focused on cyber VAT fraud investigation and digital evidence management.

5. Digital Standardisation for E-Reporting and E-Invoicing (see below)

    - Prioritise the **standardisation of digital reporting systems at the EU level,** ensuring coherence, efficiency, and low implementation burdens for businesses.
    - Ensure that implementation is proportionate, particularly for SMEs, and supported by EU-level guidance and funding mechanisms.

6. Ethical and Legal Governance of Technological Tools

    - Establish regulatory frameworks to oversee the deployment of AI and surveillance tools, **ensuring compliance with EU data protection law and maintaining public trust, in full respect of the balance of fundamental rights and in alignment with the evolving European regulatory framework on artificial intelligence.**

      AI technologies should be regulated within this normative context, not only to ensure legal and ethical oversight, but also to clarify their appropriate use in VAT fraud investigations. AI can serve as a valuable tool for anomaly detection and early-stage risk assessment; however, it must be complemented by human validation and oversight to avoid automated bias or false positives.

      The use of AI in this domain should be understood as instrumental to strengthening the guarantees of the investigative process—not replacing it—and as a means to support, rather than substitute, traditional forensic and judicial procedures.

      A key structural challenge is the absence of common datasets suitable for training and calibrating AI systems. Not only is there no EU-wide database for VAT-related investigations, but significant fragmentation also persists within individual Member States. It is therefore necessary to identify or construct interoperable baseline datasets that can support effective, accountable, and harmonised AI deployment across jurisdictions.

3.3 Effective use of reporting systems

Building on insights from both the literature and expert consultations, it is increasingly recognised that real-time reporting mechanisms—such as the Transaction Network Analysis (TNA), the VAT Information Exchange System (VIES), and the One-Stop Shop (OSS)—alongside comprehensive e-invoicing systems, constitute critical components in the prevention and early detection of cyber VAT fraud, particularly in the context of cross-border digital commerce. As highlighted by Llopis-Gilabert et al. (2022), these tools enhance fiscal transparency and reduce the latency between taxable transactions and enforcement actions, thereby limiting the window of opportunity for fraudulent conduct. Focus group discussions within this project echoed similar conclusions, stressing that the successful implementation of real-time data exchange mechanisms at the EU level would significantly strengthen the Union's ability to monitor intra-community transactions and uncover fraudulent patterns.

Additional research supports this view. Merkx and Verbaan (2019) argue that real-time access to transaction-level data allows tax authorities to move from reactive to proactive fraud detection models. Similarly, the OECD (2017) has emphasised the benefits of e-invoicing and digital reporting systems in reducing VAT compliance gaps and increasing traceability. Experts consulted during this study also highlighted the necessity of harmonising these digital infrastructures across Member States to avoid fragmentation and jurisdictional loopholes. Crucially, the burden of compliance—particularly for small and medium-sized enterprises (SMEs)—must be managed carefully to prevent unintended economic disadvantages. In this respect, simplified reporting regimes and technical support structures for SMEs are recommended.

Finally, the deterrent effect of fast and visible monitoring systems was a recurring theme in the discussions. Visible enforcement backed by technological sophistication not only improves the likelihood of detection but also reinforces taxpayer trust and voluntary compliance. These findings support the policy recommendation to accelerate the development and implementation of interoperable, real-time VAT monitoring tools at the EU level, accompanied by adequate safeguards for data protection and administrative feasibility.

In light of the above, the policy recommendations aimed at effecting using exporting systems, are as follows:

1. Accelerate the EU-Wide Implementation of Real-Time VAT Reporting Mechanisms

   The European Commission should propose a **legislative roadmap mandating minimum real-time reporting capabilities**, supported by dedicated funding for Member States' digital infrastructure upgrades.

2. Promote Harmonisation of E-Invoicing and Digital Reporting Infrastructures

   Develop a **common EU e-invoicing standard** (possibly through an update of the VAT Directive), ensuring technical compatibility and alignment with existing initiatives like PEPPOL and the ViDA (VAT in the Digital Age) proposals.

3. Transition Tax Authorities from Reactive to Proactive Fraud Detection Models

   Provide EU-wide **technical guidance and shared services** (e.g., via Eurofisc or a centralised EU platform) to lower the entry barrier for less digitally advanced tax authorities.

3.4 Judicial cooperation

A recurring theme emerging from both the expert consultations and literature review is the critical importance of harmonisation and mutual recognition mechanisms across Member States to address cyber-enabled VAT fraud effectively. While full legislative harmonisation remains complex due to the diversity of national legal systems and sovereignty concerns, national experts and researchers consistently stressed the necessity of establishing common operational standards and fostering mutual trust. This form of ***horizontal cooperation***—grounded in shared principles, interoperable procedures, and cross-border recognition of investigative actions—is essential to mitigate fragmented enforcement and enhance the effectiveness of the EU's overall fraud response.

In this context, the **pivotal role of the European Anti-Fraud Office (OLAF)** was strongly emphasised. Experts agreed that OLAF is uniquely positioned to act as a central hub for the coordination of cross-border investigative efforts and the circulation of evidence among Member States. However, to fulfil this role more effectively—especially in cases involving digital and transnational dimensions—there is a clear need to strengthen OLAF's investigative mandate, while simultaneously ensuring that such expansion respects the principles of subsidiarity and national sovereignty.

From a policy perspective, the European Commission should consider adopting a dual-track strategy. This would involve:

a) **Enhancing administrative and technical enforcement capacities at the national level**, especially in terms of technological infrastructure and data integration; and

b) **Reinforcing OLAF's operational and investigative powers**, particularly for coordinating and supporting multi-jurisdictional investigations into VAT fraud and cyber-related offences.

To achieve this, the following policy recommendations are proposed:

1. <u>Strengthen Cross-Border Investigative Cooperation</u>

    - Promote the broader and more systematic use of the **European Investigation Order (EIO)** to streamline the exchange of digital evidence and facilitate timely investigative actions across jurisdictions.
    - Encourage the development of **harmonised reporting and audit systems**, supported by unified data-sharing protocolsthat ensure compatibility and legal reliability across Member States.
    - Consider establishing **mutual recognition mechanisms for administrative and evidentiary procedures**, to avoid duplication and conflicting outcomes.

2. <u>Expand OLAF's Investigative Capacity</u>

    - Broaden OLAF's mandate to include **more proactive investigative powers**, especially in areas involving cyber-enabled fraud, while maintaining appropriate checks to safeguard national competencies.
    - Allocate targeted resources to OLAF for investment in **digital forensics, AI-driven data analytics, and secure cross-border communication tools** to support complex investigations.
    - **Facilitate joint investigation teams (JITs**) where appropriate, coordinated by OLAF and involving relevant national agencies, to improve the handling of high-risk, high-value fraud cases.

3. <u>Promote Data Integration and Interoperability</u>

Some countries highlighted the strategic need for better integration of national data systems, such as:

- Develop **centralised databases** accessible to authorised tax authorities, financial intelligence units, and law enforcement agencies, ensuring real-time information exchange. It would be very important also to enhance the exchange of tax information between revenue authorities. While these bodies are not investigative per se, they often play a key role in identifying tax fraud, and faster information exchange could significantly improve detection efforts.

- Ensure these systems are **interoperable and secure**, incorporating functionalities for automated anomaly detection and **risk assessment tools** powered by machine learning.

- Integrate multiple data sources, including **e-invoicing platforms, digital payment systems, and customs databases**, to create a comprehensive overview of transactional behaviour and detect patterns indicative of VAT fraud.

4. Balance Efficiency with Safeguards

   - Introduce **standardised audit and accountability frameworks** to govern data access and use, ensuring proportionality and protecting individual and corporate rights.

   - Offer **guidance and training** for national agencies and OLAF personnel on the ethical and legal dimensions of cross-border digital investigations.

4. Payment service providers and platform obligations

The introduction of **Directive (EU) 2020/284** represents a major development in the European Union's strategy to address VAT fraud in the rapidly evolving digital economy. The Directive requires **payment service providers (PSPs)** to collect and report detailed data on cross-border payments, including information on payers, payees, and transactions. This data is intended to be shared with national tax authorities, enabling them to better detect, monitor, and prevent VAT fraud, particularly in the context of e-commerce. Despite a general alignment, implementation has revealed **divergent approaches** to enforcement. Sanctions for non-compliance vary significantly across MSs, ranging from **administrative fines** to **criminal penalties**, including **non-monetary measures** such as public disclosure or imprisonment in severe cases. However, across the board, administrative sanctions are increasingly recognised as more **effective, proportionate, and enforceable**, especially in the context of financial transactions.

A number of critical insights emerged from the focus groups, national responses, and the literature (Merkx & Verbaan, 2019; OECD, 2017; Künnapas et al., 2025):

- **Data availability vs. processing capacity**: Many experts agreed that the key issue is not a lack of transaction data, but the limited ability of tax authorities to process, cross-reference, and extract actionable intelligence from this information. This fragmentation is evident not only across different countries but also within individual Member States, where coordination challenges often arise between domestic authorities—for instance, between the *Guardia di Finanza* and the *Agenzia delle Dogane e dei Monopoli* in Italy.
- **Proportionality of obligations**: Some MSs cautioned against over-regulating PSPs. They advocated for a balanced approach that considers the administrative burdens already borne by service providers.
- **Real-time and harmonised reporting systems**: This consideration extends to PSPs as well, in light of the demonstrated effectiveness of such instruments, as outlined above.
- **Collaboration and communication**: There was broad consensus on the necessity of fostering structured cooperation channels between PSPs and tax administrations across MSs to promote mutual trust, reduce duplication, and enhance responsiveness. For this reasons, it would be important to develop **EU-wide protocols for data sharing**, cooperation agreements, and feedback mechanisms between PSPs and national authorities, ensuring consistent standards and secure data flows.

In light of the above, the policy recommendations aimed at giving a more important role of the PSPs, are as follows:

1. Strengthen the Data Processing Capacities of Tax Authorities

   The European Commission should establish a Digital **VAT Intelligence Support Facility**, offering technical tools, shared algorithms, and analytics expertise to help Member States extract actionable insights from PSP data.

2. Promote Harmonised and Proportionate Sanctions Across Member States

   The Commission should publish **non-binding guidelines** or a Commission Recommendation outlining best practices for **proportional sanctioning and discouraging criminal penalties unless clearly justified.**

Introduce **reporting thresholds,** simplified regimes, or phased obligations for PSPs based on size, transaction volume, or risk classification.

3. Improve Domestic Inter-Agency Coordination in VAT Fraud Enforcement

   Encourage Member States to **designate a single point of contact or national coordination** unit for VAT fraud data processing and enforcement.

5. Conclusions

The fight against cyber VAT fraud, but also VAT fraud in general, requires a strategic shift from fragmented national responses to a more harmonised, intelligence-led, and technology-driven enforcement model at the EU level. While full legislative harmonisation remains complex due to divergent national legal systems, this study confirms that operational convergence, based on mutual trust and standardised practices, can significantly improve the effectiveness of cross-border investigations.

The central role of OLAF in coordinating investigations and facilitating the circulation of evidence has been widely acknowledged. However, there is a growing consensus among experts and national authorities on the need to enhance OLAF's investigative powers—especially in the digital realm—while fully respecting Member State sovereignty and the principle of subsidiarity. Strengthening OLAF's capacity must be paralleled by improved interoperability of national systems, broader use of existing tools like the European Investigation Order, and better coordination between administrative and judicial authorities.

Moreover, the obligations introduced under Directive (EU) 2020/284 for Payment Service Providers (PSPs) represent a pivotal step forward. Yet, their full potential can only be realised if these obligations are supported by harmonised administrative liability frameworks, real-time data access for authorities, and coordinated audit mechanisms across Member States. Emphasis should also be placed on proportionality: strengthening compliance and reporting without overburdening service providers or small businesses.

Finally, the conclusions of this analysis highlight three interrelated pillars for future policy development:

1. **Enhanced Horizontal Cooperation** – Through common standards, shared investigative practices, and mutual recognition of evidence, Member States can move toward operational harmonisation without requiring deep legislative change.
2. **Technological and Institutional Integration** – From centralised databases to AI-driven risk analysis tools, the integration of digital infrastructure must underpin VAT fraud prevention and enforcement across the EU.
3. **Balanced and Coordinated Enforcement** – A dual-track approach that reinforces both national administrative enforcement and EU-level investigative coordination will strengthen the overall integrity of the Union's financial interests.

In conclusion, effective prevention and repression of cyber VAT fraud will depend not on the proliferation of new offences, but on the smarter, more collaborative use of existing tools and competencies. Policymakers are therefore encouraged to invest in coordination, data-driven enforcement, and capacity building at both national and European levels.

Recommendations | Summary

Three Interrelated Pillars for Future Policy Development

Enhanced Horizontal Cooperation

Through common standards, shared investigative practices, and mutual recognition of evidence, EU Member States can move toward operational harmonisation without requiring deep legislative change.

Technological and Institutional Integration

From centralised databases to AI-driven risk analysis tools, the integration of digital infrastructure must underpin VAT fraud prevention and enforcement across the EU.

Balanced and Coordinated Enforcement

A dual-track approach that reinforces both national administrative enforcement and EU-level investigative coordination will strengthen the overall integr ity of the Union's financial interests.

Harmonisation, Legal Convergence and Integration in the EU

- Strengthen enforcement and monitoring of the PIF Directive
- Promote further harmonisation of the subjective element of the VAT-related offences
- Ensure pacific aggravating circumstances for organised VAT fraud
- Institutionalise peer-learning and knowledge-sharing platforms
- Broaden and systematise stakeholder engagement

Regulatory Reforms

- Do not introduce a separate offence for cyber VAT fraud
- Harmonise the definition of VAT fraud at the EU level
- Consider cyber elements as aggravating circu mstances
- Prioritise investment in investigative and technological capacities
- Strengthen administrative liability regimes for legal persons
- Explore fiscal policy measures such as sector-specific split payment regimes

Investigations

- Develop minimum standards for institutional capacity
- Promote EU-wide specialised training and curricula
- Enhance procedural harmonisation
- Encourage the establishment of special ised judicial tracks
- Align statutes of limitations with complexity of transnational crime

Use of Technology in Prevention and Investigations

- Technological modernisation of investigative tools
- Interconnection of National data systems
- Harmonisation of digital infrastructures
- Specialised Training and dedicated Units
- Digital standardisation for E-Reporting and E-Invoicing
- Ethical and Legal Governance of technological tools

Use of Reporting Systems

- Accelerate the EU-Wide implementation of Real-Time VAT Reporting Mechanisms
- Promote Harmonisation of E-Invoicing and Digital Reporting Infrastructures
- Transition Tax Authorities from reactive to proactive fraud detection models

Judicial Cooperation

- Strengthen Cross-Border investigative cooperation
- Expand OLAF's investigative capacity
- Promote Data integration and interoperability
- Balance efficiency with safeguards

Payment Service Providers and Platform Obligations

- Strengthen the data processing capacities of Tax Authorities
- Promote harmonised and proportionate sanctions across Member States
- Improve domestic Inter-Agency coordination in VAT Fraud Enforcement

Bibliography

Bernardi, A., & Negri, D. (Eds.). (2015). *Relationships between the national judicial authorities and the investigative agencies in the view of the EPPO: Operational models and best practices in fight against EU frauds (Booklet of the research, February – June 2015)*. University of Ferrara. Project financed by the European Commission – OLAF, Hercule III Programme (OLAF/2015/D1/006). Accessible at: http://www.unife.it/progetto/olaf

Farkas, Á., Dannecker, G., & Jacsó, J. (Eds.). (2019). *Criminal law aspects of the protection of the financial interests of the European Union: With particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*. Wolters Kluwer Hungary Kft.

Foffani, L., Bin, L., & Carriero, M. F. (Eds.). (2019). *Cyber VAT frauds, ne bis in idem and judicial cooperation: A comparative study between Italy, Belgium, Spain and Germany*. Giappichelli Editore. (Progetto finanziato dal programma HERCULE III dell'Unione Europea: EUROPE AGAINST CYBER VAT FRAUDS – EACVF)

Lasagni, G. (2015). Cooperazione amministrativa e circolazione probatoria nelle frodi doganali e fiscali: Il ruolo dell'Ufficio europeo per la lotta antifrode (OLAF) alla luce della direttiva OEI e del progetto EPPO. *Diritto Penale Contemporaneo*.

Llopis-Gilabert, B., Leal-Buenfil, R., & Pla-Julián, I. (2022). Fiscal and economic competition implications of carousel fraud in the European Union. *International Journal of Business & Management Studies, 3*(5).

Merkx, M., & Verbaan, N. (2019). Technology: A key to solve VAT fraud? *EC Tax Review, 28*(6), Kluwer Law International BV, 326-332.

OECD. (2017). *Technology Tools to Tackle Tax Evasion and Tax Fraud*. OECD Publishing.

Künnapas, K., Maslionkina, P., Hinno, R., & Liberts, R. (2025). Current AI applications by Estonian tax authorities and use case scenarios. *TalTech Journal of European Studies, 15*(1[41]). https://doi.org/10.2478/bjes-2025-0010