MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Criminology Investigation & Justice
ISSN: 3064-7940

Combating Cyber VAT Fraud in the EU Member States: A Comparative Study of Criminal and Criminal Procedure Law

Baratto G[1,3], Boriero D[3], Di Nicola A[1,3]*, Flor R[2,3], Panattoni B[2] and Perrone G[1,3]

[1]Faculty of Law, University of Trento, Italy
[2]Department of Law, University of Verona, Italy
[3]Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy

***Corresponding author:** Andrea Di Nicola, Faculty of Law, University of Trento, Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy, Email: andrea.dinicola@unitn.it

Research Article
Volume 3 Issue 1
Received Date: January 15, 2025
Published Date: January 31, 2025
DOI: 10.23880/oajcij-16000130

Abstract

VAT fraud has long posed a major challenge to the economic stability of individual countries and the European Union (EU) as a whole. In recent years, the convergence of VAT fraud and cybercrime has led to a new phenomenon: cyber VAT fraud. Despite its increasing prevalence, this complex issue has not yet been sufficiently researched and a comprehensive framework to combat it effectively has yet to be developed.

This article is an anticipation of the comparative legal analysis on combating cyber VAT fraud in the European Union, which is part of the project "EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study", co-founded by the Union Anti-Fraud Program (EUAF) of the European Anti-Fraud Office (OLAF).

The EU CYBER VAT project aims to fill this gap by assessing the adequacy of the existing legal framework both at EU and Member State level. The comparative analysis examines whether the current rules, including the PIF Directive and its implementation at national level, provide solid and effective protection against the new threats posed by cyber VAT fraud.

Keywords: Value-Added Tax; VAT Fraud; Cybercrime; Cyber VAT Fraud; EPPO; European Union

Abbreviations

VAT: Value Added Tax; EPPO: European Public Prosecutor's Office; EU: European Union; ICT: Information and Communication Technology; CSSC: Centre of Security and Crime Science; OSS: One Stop Shop; PSPs: Payment Service Providers; AI: Artificial Intelligence.

Introduction

It is well known that VAT fraud is a phenomenon that has always seriously affected the economies of individual countries and the European Union. In fact, value added tax (VAT) is one of the most important components of public revenue and represents an essential source of own resources for both the EU budget and national budgets. The importance of VAT goes beyond its role as a mere tax; it is a key element of the financial framework that sustains the European project, finances public services and facilitates cross-border trade in the internal market[1] [1]. The significant impact of fraud

1 Among the various contributions, see for instance: M.C. Frunza, "Value Added Tax Fraud", Routledge, 2018; S. Fedeli, F. Forte, "EU VAT Fraud", in European Journal of Law and Economics, Vol. 31, n. 2, 143-166, 2009; M. Keen, S. Smith, "VAT Fraud and Evasion: What Do We Know and What Can Be Done?" in National Tax Journal, Vol. 59, n. 4, 861-887, 2006. To better understand the European dimension of this crime, see: M. Griffioen,

on European financial interests led to the establishment of the European Public Prosecutor's Office (EPPO) in 2020, which became operational on July 1, 2021. It was established on the basis of Council Regulation (EU) 2017/1939, which was adopted on October 12, 2017, as part of the enhanced cooperation between the participating EU Member States.

The EPPO operates as an independent body that ensures a coordinated and efficient approach to combating cross-border financial crime that undermines the EU budget and the integrity of the EU's financial systems.

The EPPO's mission is to protect the financial interests of the European Union by investigating, prosecuting and bringing to justice crimes that undermine the economic integrity of the Union. These crimes include large-scale VAT fraud, corruption, money laundering and the misappropriation of EU funds. By prosecuting these serious financial crimes, the EPPO plays an important role in ensuring accountability, protecting taxpayers' money and maintaining trust in the EU institutions.

On February 29, 2024, the EPPO published its annual report for the year 2023, outlining the scope and impact of its activities. During the year, the EPPO opened 1,371 investigations, with total estimated losses amounting to €19.2 billion. Of particular note is that €11.5 billion - or 59% of the total - was related to serious VAT fraud, highlighting the scale of the problem. This figure represents a 71% increase on the VAT-related losses reported in 2022[2] [2], reinforcing the ability and awareness of institutions such as the EPPO in detecting and combating these crimes, but also highlighting the increasing sophistication and scale of such fraudulent activity.

In recent years, criminals have increasingly taken advantage of technological advances to commit various types of crime, including financial crime and VAT fraud in particular[3] [3]. The emergence of digital technologies has opened up new avenues for fraudulent activity, making it more difficult for authorities to detect and prevent such crimes[4] [4]. Understanding the role of information and communication technology (ICT) in cyber VAT fraud is critical to countering the new threats posed by the digitization of tax operations. A thorough understanding of these dynamics is key to developing targeted, proactive law enforcement strategies[5] [5]. This knowledge not only helps to identify best practice in the fight against cyber VAT fraud, but also forms the basis for effective cooperation between Member States. The efforts of the European Public Prosecutor's Office and other European and supranational institutions, such as Europol, can be significantly strengthened by a unified approach. This will enable a faster and more effective response to the increasing complexity of financial crime and ensure that perpetrators are brought to justice.

Furthermore, these efforts are in line with the political guidelines for the next European Commission (2024–2029), which emphasize the importance of strengthening the EPPO's capacities. The guidelines foresee that the EPPO will be given more powers and receive more support from Europol, which is expected to develop into a fully operational police authority and significantly increase its staff over time[6] [6].

E.C.J.M. van der Hel-van Dijk "Tackling VAT-Fraud in Europe: A Complicated International Puzzle", in Intertax, Volume 44, Issue 4, 290 – 297, 2016; L. Sergiou, "Value Added Tax (VAT) Carousel Fraud in the European Union" in Journal of Accounting and Management, vol. 2 n. 2, 9-21, 2012, M. Lamensch, E. Ceci, "VAT fraud - Economic impact, challenges and policy issues", Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, 2018, retrieved from: https://www.europarl.europa.eu/cmsdata/156408/VAT%20Fraud%20Study%20publication.pdf; F. Borselli, "Organised Vat Fraud: Features, Magnitude, Policy Perspectives", in Bank of Italy Occasional Paper No. 106, 2011, retrieved from: https://ssrn.com/abstract=1966015; R. F. van Brederode, "Third-Party Risks and Liabilities in Case of VAT Fraud in the EU", in International Tax Journal, January – February, 2008, 31-42; M. Frunza, "Cost of the MTIC VAT Fraud for European Union Members", 2016, retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2758566; T. Michalik, "How the European Commission and European Countries Fight VAT Fraud", mBank - CASE Seminar Proceedings 0147, CASE-Center for Social and Economic Research, 2017;

2 EPPO Annual Report 2023, retrieved from: https://www.eppo.europa.eu/sites/default/files/2024-03/EPPO_Annual_Report_2023.pdf; J. Sarnowski, P. Selera, "European compact against tax fraud—VAT solidarity and new dimension of effective and coherent tax data transfer", ERA Forum 21, 2020, p. 81–93, retrieved from: https://doi.org/10.1007/s12027-020-00603-z;

3 On digital VAT frauds, see: L. Foffani, L. Bin, M. F. Carriero, "Cyber VAT frauds, ne bis in idem and judicial cooperation, A comparative study between Italy, Belgium, Spain and Germany" – Research project, Giappichelli, 2019; J. Nicholls, A. Kuppa and N. A. Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," in IEEE Access, vol. 9, 163965-163986, 2021; M. Lagazio, N. Sherif, N. Cushman, "A multilevel approach to understanding the impact of cyber crime in the financial sector" in Computer & Security, Vol. 45, 1-32, 2014; J. Vanhoeyveld, D. Martens, B. Peeters, "Value-Added Tax fraud detection with scalable anomaly detection techniques" in Applied Soft Computing, Vol. 86, n. , 2020; F. Borselli, S. Fedeli, L. Giuriato, "Digital VAT carousel frauds: a new boundary for criminality?", TAX NOTES INTERNATIONAL; 707-724, 2015; Papis-Almansa, "VAT and electronic commerce: the new rules as a means for simplification, combatting fraud and creating a more level playing field?", ERA Forum 20, 2019, 201–223, retrieved from: https://doi.org/10.1007/s12027-019-00575-9; R. T. Ainsworth, "Carousel Fraud in the EU: A Digital Vat Solution", in Tax Notes International, p. 443, May 1, 2006, Boston Univ. School of Law Working Paper No. 06-23, retrieved from: https://ssrn.com/abstract=924189

4 F. Borselli, "Pragmatic Policies to Tackle VAT Fraud in the European Union" in International VAT Monitor, No. 5, 332-343, September/October 2008; O. Sokolovska, "Cross-border VAT frauds and measures to tackle them", 2016, retrieved from: ttps://mpra.ub.uni-muenchen.de/70504/ ; European Union, "Tackling intra-Community VAT fraud: More action needed", Publications Office of the European Union, 2016.

5 CESOP - Guidelines for the reporting of payment data, 2023, retrieved from: https://taxation-customs.ec.europa.eu/taxation/vat/fight-against-vat-fraud/tackling-vat-fraud-e-commerce-cesop_en

6 Ursula von der Leyen, Candidate for the European Commission President, EUROPE'S CHOICE - POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2024–2029, retrieved from: https://

This enhanced institutional cooperation will enable more efficient and coordinated action to combat complex fraud and related crimes across Europe.

However, it is clear that in order to achieve these objectives, accurate and shared data on what is happening in each Member State is needed, at least at European level. To meet this need, the Centre of Security and Crime Science (CSSC) has launched the EU CYBER VAT research project[7] [7].

This article is an anticipation of the comparative legal analysis on combating cyber VAT fraud in the European Union, carried out in the project.

The Project EU CYBER VAT: Objectives and Methodology

Despite the widespread prevalence of cyber VAT fraud and its significant impact on the global economy, the literature on the subject - both in criminal law and criminology - remains remarkably sparse and incomplete. The phenomenon has not yet been extensively studied and there is a notable lack of a coherent account of the criminal law and procedural tools to combat it effectively.

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 the fight against cyber VAT fraud and to propose solutions to make it more effective and efficient at EU and Member State level. Using the comparative law research method, the project examines 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 overlap of VAT fraud and cybercrime. As these are cross-border and particularly serious crimes, it is, as already emphasized, crucial to monitor and ensure a high level of harmonization between national rules.

The existing gap is further highlighted by the lack of a common and standardized definition of cyber VAT fraud. For the purposes of this article, we adopt the definition used in the EU CYBER VAT project:

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.

As you can see, this definition is broad. It is a criminological definition that focuses on the phenomenon and is not strictly bound to the description of a specific offense. It also does not describe the individual acts that make up a typical criminal offense. This definition encompasses different acts and different types of crime. It does not refer to a specific cybercrime in the narrow sense, but to a cybercrime in a broader sense. It includes all cases in which the technology facilitates or supports the commission of the offense. This means that, in addition to national regulations on VAT fraud and EU law - in particular Directive 2006/112/EC (VAT Directive), Council Regulation (EU) No. 904/2010, Directive (EU) 2017/1371 (PIF Directive) and Directive 2018/822 (DAC 6) - the 2001 Council of Europe Convention on Cybercrime (commonly known as the Cybercrime Convention or Budapest Convention) also applies. This is particularly due to the fact that the procedural part (Articles 9-13) and the third part on international cooperation (Articles 14-17) apply not only to the crimes defined in the Convention itself, but also to crimes committed by technical means and to the procedures for collecting and processing digital evidence.

As will be seen later, this phenomenological definition is sufficient for the fight against cyber VAT fraud, as it is not necessary to define a new specific offense.

The methodology applied in the project started with a comprehensive inventory of substantive and procedural criminal law in all EU Member States in relation to the fight against VAT fraud.

To answer the research questions, a detailed questionnaire was distributed to one national expert from each Member State (MS), all from academia. Subsequently, two focus groups were convened to discuss the preliminary results of the questionnaire. These discussions were attended not only by the national experts, but also by key stakeholders, including prosecutors and law enforcement agencies. Finally, the experts and stakeholders were invited to present national case studies on cyber VAT fraud and provide their assessments of proposals, suggestions and best practices to improve responses to this growing problem.

The most important ongoing results of the project in relation to criminal law and criminal procedure are presented below[8] [8].

commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

7 Research project EU CYBER VAT: - *Fighting Cyber-VAT Fraud in the EU: A Comparative Criminological and Criminal Law Study,* co-funded by the EU Anti-Fraud Programme (EUAF), conducted by the Centre for Security and Crime Sciences (CSSC), University of Trento and University of Verona;

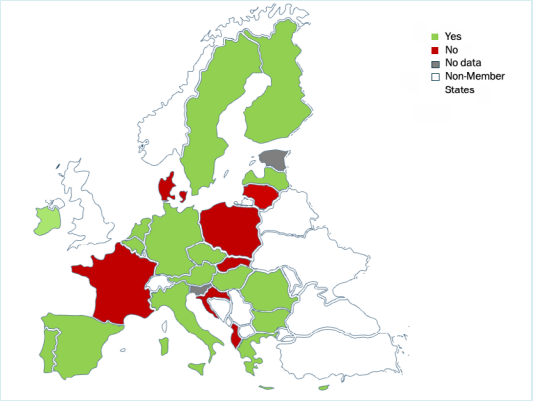
8 Data has been collected from 25 of the 27 Member States, with Slovenia and Estonia being the exceptions.

The Project EU CYBER VAT: Results

According to the replies, the PIF Directive has been correctly transposed in most Member States, so that all provisions are covered. In most cases, this required amendments to existing legislation, as the previous laws were not as comprehensive as the Directive and did not meet its minimum standards.

With regard to Article 3 of the Directive, which defines specific criminal offenses affecting the EU's financial interests[9] [9], most Member States (20 out of 25 respondents) have fully complied with the requirements. However, five countries (Croatia, Denmark, France, Lithuania and Slovakia) have not fully transposed the Directive (Figures 1-3).

- due to its opt-out, Denmark was not legally obliged to transpose the directive, but is still bound by the PIF Convention;
- Croatia, Lithuania and Slovakia have partially amended their existing laws, but still do not meet the requirements of the Directive;
- France has not yet amended its legislation at all.

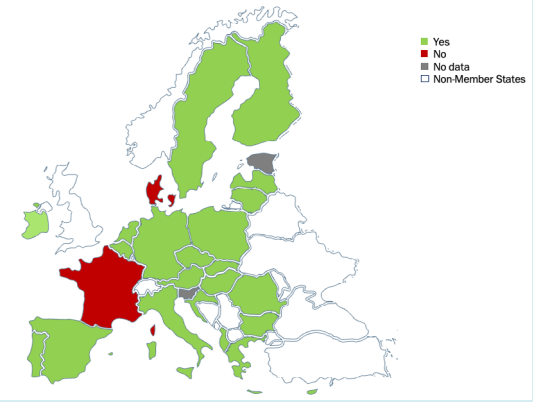


Source: elaboration by CSSC of the responses collected through experts' questionnaires – project EU CYBER VAT
Figure 1: MSs Compliance with Article 3 PIF Directive.

In addition, almost all Member States provide for the liability of legal persons for this type of offense in accordance with Article 6 of the PIF Directive. Most countries already had such provisions in place before the adoption of the Directive. Thus, 23 out of 25 Member States have correctly implemented these provisions.

The two exceptions are:

- Denmark, which is not legally obliged to transpose the Directive, but has acceded to the PIF Convention.
- France, which has not yet made the necessary legislative changes.

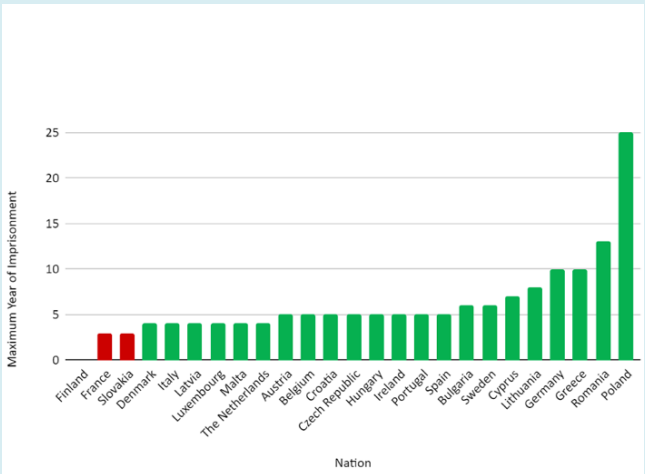


Source: elaboration by CSSC of the responses collected through experts' questionnaires – project EU CYBER VAT
Figure 2: Compliance with Art. 6 PIF Directive.

9 Article 3, par. 2:
2. For the purposes of this Directive, the following shall be regarded as fraud affecting the Union's financial interests:
(a) in respect of non-procurement-related expenditure, any act or omission relating to:
(i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds or assets from the Union budget or budgets managed by the Union, or on its behalf;
(ii) non-disclosure of information in violation of a specific obligation, with the same effect; or
(iii) the misapplication of such funds or assets for purposes other than those for which they were originally granted;
(b) in respect of procurement-related expenditure, at least when committed in order to make an unlawful gain for the perpetrator or another by causing a loss to the Union's financial interests, any act or omission relating to:
(i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds or assets from the Union budget or budgets managed by the Union, or on its behalf;
(ii) non-disclosure of information in violation of a specific obligation, with the same effect; or
(iii) the misapplication of such funds or assets for purposes other than those for which they were originally granted, which damages the Union's financial interests;
(c) in respect of revenue other than revenue arising from VAT own resources referred to in point (d), any act or omission relating to: (i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the Union budget or budgets managed by the Union, or on its behalf;
(ii) non-disclosure of information in violation of a specific obligation, with the same effect; or
(iii) misapplication of a legally obtained benefit, with the same effect;
(d) in respect of revenue arising from VAT own resources, any act or omission committed in cross-border fraudulent schemes in relation to:
(i) the use or presentation of false, incorrect or incomplete VAT-related statements or documents, which has as an effect the diminution of the resources of the Union budget;
(ii) non-disclosure of VAT-related information in violation of a specific obligation, with the same effect; or
(iii) the presentation of correct VAT-related statements for the purposes of fraudulently disguising the non-payment or wrongful creation of rights to VAT refunds.

Similar trends are emerging with reference to EU Directive 2020/284, which deals with the general obligations for payment service providers and the MOSS system (Mini One-Stop Shop). Most Member States have implemented the requirements of the Directive, ensuring greater harmonization and compliance in these areas. As regards the distinction between VAT fraud and cyber VAT fraud in national legal systems, it is noteworthy that only Cyprus has introduced specific legislation to combat cyber VAT fraud. In contrast, most other Member States treat this type of offense under the broader category of VAT fraud or more generally under the umbrella term of tax evasion. This leads to the first point: in most Member States, not only is there no specific offense for cyber VAT fraud, but in several cases there is also no separate, standalone offense explicitly dedicated to VAT fraud itself. Instead, such offenses are often subsumed under broader legal frameworks that may lack the necessary precision to capture the specific characteristics of VAT fraud. While VAT fraud is a subset of tax evasion, it focuses exclusively on the mechanics of VAT and therefore requires specific strategies to combat it effectively. As far as the subjective element is concerned, three quarters of the responding countries (17 out of 25) provide for criminal liability only in cases of intent. None of the Member States provide for exclusive criminal liability for negligence (culpa), while seven states provide for liability for both intent and negligence (Cyprus, Denmark, Finland, Germany, Malta, Romania, the Netherlands and Sweden). As regards compliance with the sanctions required by Article 7 of the PIF Directive, in particular the setting of a maximum penalty of at least four years' imprisonment in cases where the fraud affecting the EU's financial interests results in damage of more than EUR 100 000 (the threshold for "significant damage"), only two Member States - France and Slovakia - still impose a maximum penalty of less than four years in such cases. In the case of Greece, national legislation does not provide for a maximum penalty, but a minimum penalty of 10 years. In Finland, although the maximum penalty for VAT fraud is two years' imprisonment, compliance with Article 7 of the VAT Directive appears to be ensured by the combined application of other provisions of the Finnish Criminal Code.

Compliance with sanctions in relation to legal persons is primarily of a criminal nature, although there are also non-criminal (administrative or civil) sanctions. Many of the responding Member States provide for the sanctions referred to in Article 9[10] [10] of the PIF Directive, either in full or in part.



Source: elaboration by CSSC of the responses collected through experts' questionnaires – project EU CYBER VAT

Figure 3: Compliance with article 7 PIF Directive: compliance with required maximum sentence.

The final aspect in relation to substantive criminal law was the assessment of compliance with Article 8 of the Directive, which refers to the establishment of an aggravating circumstance for the commission of VAT fraud in the context of organised crime: 22 out of 25 countries provide for this. Most Member States also show a high level of compliance with regard to procedural aspects. In particular, Article 11, which refers to national jurisdiction, and Article 12, which deals with limitation periods, were examined.

Law enforcement authorities in the EU use a variety of investigative tools and measures to combat VAT fraud, adapting their strategies to the local legal framework but also adopting common approaches between Member States. Experts representing each EU Member State gave an insight into the specific methods available to their respective law enforcement authorities [11].

The most important methods include:

- **Data analysis and information sharing:** many authorities rely on data analysis, information sharing and automated verification systems (such as the VIES in

10 Article 9: Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 6 is subject to effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions, such as:
(a)exclusion from entitlement to public benefits or aid;
(b)temporary or permanent exclusion from public tender procedures;
(c) temporary or permanent disqualification from the practice of commercial activities;
(d)placing under judicial supervision;
(e)judicial winding-up;
(f) temporary or permanent closure of establishments which have been used for committing the criminal offence.

Malta and the Czech Republic) to detect inconsistencies and patterns indicative of VAT fraud;

- **Audits and inspections:** routine audits and inspections are fundamental tools. These checks are often done on a random basis, but a risk-based approach can be used to conduct targeted audits if prior analysis identifies inconsistencies;
- **Search and seizure:** in many countries, as for instance Bulgaria, Ireland, and The Netherlands, search and seizure measures are carried out, often focusing on digital evidence to gather physical evidence of fraudulent activity;
- **Interviews, audits and surveillance:** investigative measures such as interrogations, interviews and surveillance are often used to monitor suspicious activity and gather witness statements. Not only the suspect is questioned, but also experts and witnesses such as co-workers;
- **Cooperation with other agencies:** international cooperation and collaboration with other agencies and financial police increase the effectiveness of investigations by sharing intelligence and resources. States are well aware of the complexity and internationalisation of this type of crime; therefore, they are introducing new ways of sharing information and putting together new agencies and data channels to monitor compliance in a more integrated manner;
- **Coercive measures:** some Member States, as for instance Malta, Lithuania and Sweden, are using coercive measures such as provisional arrests and sting operations to control suspects and gather evidence discreetly (Table 1).

	MT	IE	GR	ES	RO	LU	CZ	FR	BE	HR	NL	LV	BG	LT	SE	AT	PT	DK	IT
Data Analysis and Info Sharing	X	X	X	X	X	X	X	X	X	X	X	X							X
Audits and Inspections	X	X	X		X	X		X					X					X	X
Search and Seizure	X	X									X		X	X	X	X			X
Interviews and Surveillance		X	X					X		X	X		X	X					X
Collaboration with other agencies		X	X	X		X	X	X	X	X	X	X					X		X
Coercive Measures	X													X	X				

Source: elaboration by CSSC of the responses collected through experts' questionnaires – project EU CYBER VAT
Table 1: Investigative tools/measures to detect VAT fraud.

In general, it can be observed in all European countries that the investigative tools and measures used for general VAT fraud also apply to cyber VAT fraud, so that specific tools tailored to cyber VAT fraud are very rare: several countries (Malta, Hungary, Italy, Ireland, Lithuania, Bulgaria, Spain, Slovakia, Romania, Luxembourg, Czech Republic and Belgium) report that there are no specific tools for cyber VAT fraud, suggesting a reliance on general fraud investigation tools. Latvia refers to the continuous commitment to the development of expertise and the exchange of best practices between jurisdictions, managing to adapt "traditional" strategies to today's phenomenon [12-15].

Lithuania, Sweden, Croatia and Greece emphasize the use of covert surveillance, secret monitoring of electronic communications and digital forensic analysis as effective measures. In Greece, the law allows unhindered access to various documents and data for auditing bodies and prosecutorial authorities.

Some Member States, such as Malta, have made significant investments in artificial intelligence (AI) to improve their ability to detect and combat cyber VAT fraud. The same applies to Poland, Austria and Greece [16]. These systems use advanced machine learning algorithms to analyze large data sets on taxpayers' activities in depth to detect suspicious transactions and violations of tax regulations. By identifying anomalies and atypical behaviours in real time, artificial intelligence plays a critical role in detecting irregular trading patterns, with a focus on missing trader fraud [17-19].

In general, there is a convergence between the investigative tools used for traditional VAT fraud and those used for cybercrime more broadly. In addition, the rules on the collection of digital evidence also come into play. These rules in the Member States are often derived from European instruments, such as the Budapest Convention on Cybercrime. The main proposals put forward by experts and stakeholders to improve investigative tools to combat cyber VAT fraud

include, in particular, the need for specialized training for professionals and the strengthening of cooperation between Member States and competent authorities [20-22].

In detail, the proposals include:

- **Inter-agency cooperation:** better cooperation between the different agencies and authorities responsible for detecting and investigating VAT fraud is highlighted by Greece and Bulgaria as crucial for effective enforcement;
- **Use of technology:** the introduction of new technologies such as AI to detect fraud patterns (Portugal) and digital reporting systems (Denmark) is seen as essential to modernise the fight against VAT fraud. Italy emphasises the importance of using technological tools to connect all existing databases in order to perform cross-checks of data. But also the invoicing and monitoring of transactions in real time;
- **Legal and procedural reforms:** countries such as Spain and France are calling for significant legal reforms, including the updating of criminal procedure laws, the extension of investigation periods and the creation of specialised courts or legal provisions specifically targeting economic and VAT fraud;
- **Effective use of data:** Romania and Slovakia point to the need for better use of existing data and reporting systems by tax authorities to more effectively detect and combat VAT fraud; Croatia agrees and proposes the creation of a central database collecting information from tax authorities, institutions and law enforcement agencies;
- **Systematic improvements:** Spain proposes a more profound change to the procedural model where prosecutors lead investigations and the need for reforms to reduce delays in complex white-collar crime cases;
- **International cooperation:** improving international cooperation and aligning with EU directives and instruments, such as the European Investigation Order, is seen as beneficial by countries such as Greece and Bulgaria;
- **Alignment of sanctions:** Malta points to the need to align criminal and administrative sanctioning procedures and to ensure that criminal proceedings are justified and meet a materiality threshold.

The need for greater harmonization and cooperation is also evident in relation to the very different systems for electronic invoicing and electronic reporting in the European Member States. The EU itself has emphasized[11] that the promotion and introduction of digital reporting obligations — optimized through the use of digital technologies and supported by minimum standards for all EU countries — would be an effective means of combating VAT and cyber VAT fraud. The experts involved generally agreed with this proposal, although some expressed concerns about the potentially excessive costs of digitalization for small traders and entrepreneurs, who could again find themselves at a disadvantage compared to larger businesses [23-25].

One of the most discussed points was the possibility of introducing new obligations for platforms and marketplaces. In most cases, however, the experts were against the introduction of additional regulations in this area, as they believe that the existing framework is already very restrictive and sufficient to ensure the accountability of platforms. For some experts, it is clear that the main problem is not the lack of information, but the ability of tax authorities to process and interpret the huge amounts of data already provided.

Finally, the last part of the questionnaire was dedicated to cyber VAT fraud in the context of e-commerce, analyzing the implementation of Directive 2020/284 and the MOSS scheme. With the exception of France, all respondents comply with Directive EU 2020/284, which introduces new rules for payment service providers (PSPs). In the event of a breach of these obligations, a range of administrative and criminal sanctions, fines and legal consequences are provided for. As a rule, the Member States impose fines, the amount of which depends on the severity and frequency of the infringement.

The MOSS (Mini One Stop Shop) scheme has been introduced in almost all Member States, with the exception of Poland and Slovakia. Services previously covered by the MOSS scheme are now covered by the One Stop Shop (OSS).

Conclusion

While the introduction of a separate offense for VAT fraud, distinct from general tax evasion, may be justified, the introduction of a specific offense for cyber VAT fraud does not seem necessary. This means that the creation of a new stand-alone offense with a structural technical element is not strictly necessary, as the existing "traditional" legislation is perfectly sufficient. This conclusion is based on several considerations. From a phenomenological point of view, the definition chosen for this project is intentionally broad in order to cover a wide range of scenarios, including those involving digital elements. It is important to note that VAT fraud is classified as a "free-form" offense in most jurisdictions. This classification implies that the commission is not restricted to a limited or exhaustive list of specific acts. As a result, the inclusion of digital tools or methods in the commission of VAT fraud does not preclude it from being

11 Economisti Associati, Oxford Research, CASE, Wavestone, Hedeos, Mazars, Desmeytere Services and Universitàdi Urbino, Final report VAT in the Digital Age - Volume 1 - Digital Reporting Requirements, 2022, retrieved from: https://taxation-customs.ec.europa.eu/document/download/b09cd7eb-87ae-4317-beb8-4c0921d31353_en?filename=VAT%20in%20the%20Digital%20Age_Final%20Report%20Volume%201.pdf

prosecuted under the traditional VAT fraud legal framework. This flexible approach ensures that emerging technological dimensions of the offense are adequately addressed without the need to create a separate legal provision.

According to most experts, the introduction of an aggravating circumstance for the use of digital means would also not add significant value, as it is a natural evolution of traditional VAT fraud. The use of technology in this context does not lead to a significant increase in harmfulness or disvalue. Instead, it might be more appropriate to adapt the sanctions to the severity and scope of the offense.

However, it is necessary to focus less on the substantive aspects of criminal law and more on the procedural aspects. Attention should be paid to the discovery and collection of evidence. To combat this phenomenon effectively, it must be intercepted in real time, given the speed of transactions and the ease with which companies can be opened and closed, facilitated by technological progress.

At the same time, it seems more appropriate to strengthen cooperation between the public and private sectors in this area, rather than increasing the obligations of the platforms. Indeed, the platforms take on a quasi-public role when they cooperate with the authorities in data management.

Financial investigations involving all types of crime require the development and harmonization of new tools at European level, but also the use of intelligence systems as a method of data collection and analysis. The use of both proactive and reactive ICT strategies appears to be essential in the fight against VAT fraud and cyber VAT fraud.

The key challenge is not only to collect more data, as a significant amount is already available, but rather to analyze and compare this data in real time. Automated analysis systems that are able to detect anomalies are crucial. To achieve this, the development of artificial intelligence tools is crucial, as is already being implemented in some Member States.

Conflict of interest

The authors declare no conflict of interest.

Acknowledgement

“Project EU CYBER VAT. 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.”

References

1. Ainsworth RT (2006) Carousel Fraud in the EU: A Digital Vat Solution. Tax Notes International, pp: 443-448.
2. Borselli F, Fedeli S, Giuriato L (2015) Digital VAT carousel frauds: a new boundary for criminality? Tax Notes International, pp: 707-724.
3. Borselli F (2011) Organised Vat Fraud: Features, Magnitude, Policy Perspectives, in Bank of Italy Occasional, pp: 106.
4. Borselli F (2008) Pragmatic Policies to Tackle VAT Fraud in the European Union. International VAT Monitor (5): 332-343.
5. CESOP (2023) Guidelines for the reporting of payment data.
6. (2022) Final report VAT in the Digital Age-Volume 1-Digital Reporting Requirements. Desmeytere Services and Universita□ di Urbino, Economisti Associati, Oxford Research, CASE, Wavestone, Hedeos, Mazars.
7. EPPO (2023) Annual Report.
8. European Union (2016) Tackling intra-Community VAT fraud: More action needed. Publications Office of the European Union.
9. Fedeli S, Forte F (2009) EU VAT Fraud. European Law and Economics 31(2): 143-166.
10. Foffani L, Bin L, Carriero MF (2019) Cyber VAT frauds, ne bis in idem and judicial cooperation, A comparative study between Italy, Belgium, Spain and Germany, Research project, Giappichelli.
11. Frunza MC (2018) Value Added Tax Fraud. 1st (Edn.), Routledge, New York, USA.
12. Frunza M (2016) Cost of the MTIC VAT Fraud for European Union Members. Cost of the MTIC VAT Fraud for European Union Members.
13. Griffioen M, van der Hel-van Dijk, ECJM (2016) Tackling VAT-Fraud in Europe: A Complicated International Puzzle. Intertax 44(4): 290-297.
14. Keen M, Smith S (2006) VAT Fraud and Evasion: What Do We Know and What Can Be Done? National Tax Journal 59(4): 861-887.
15. Lagazio M, Sherif N, Cushman N (2014) A multilevel approach to understanding the impact of cybercrime in the financial sector. Computer & Security 45: 1-32.
16. Lamensch M, Ceci E (2018) VAT fraud - Economic

impact, challenges and policy issues. Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies.

17. Michalik T (2017) How the European Commission and European Countries Fight VAT Fraud. Bank - CASE Seminar Proceedings 0147, CASE-Center for Social and Economic Research.

18. Nicholls J, Kuppa A, Le-Khac NA (2021) Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. IEEE Access 9: 163965-163986.

19. Papis-Almansa M (2019) VAT and electronic commerce: the new rules as a means for simplification, combatting fraud and creating a more level playing field? ERA Forum 20: 201-223.

20. Sergiou L (2012) Value Added Tax (VAT) Carousel Fraud in the European Union. Journal of Accounting and Management 2(2): 9-21.

21. Sarnowski J, Selera P (2021) European compact against tax fraud-VAT solidarity and new dimension of effective and coherent tax data transfer. ERA Forum 21: 81-93.

22. Sokolovska O (2016) Cross-border VAT frauds and measures to tackle them.

23. van Brederode RF (2008) Third-Party Risks and Liabilities in Case of VAT Fraud in the EU. International Tax Journal, pp: 31-42.

24. von der Leyen U (2024) Candidate for the European Commission President, Europe's choice - political guidelines for the next european commission 2024-2029.

25. Vanhoeyveld J, Martens D, Peeters B (2020) Value-Added Tax fraud detection with scalable anomaly detection techniques. Applied Soft Computing, pp: 86.