ELI
EUROPEAN
LAW
INSTITUTE

Response to the European Commission's Public Consultation on the European Commission's White Paper for the Anti-fraud Architecture Review

European Law Institute

The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment, it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

President: Teresa Rodríguez de las Heras Ballell
First Vice-President: Sir Geoffrey Vos
Second Vice-President: Pietro Sirena
Treasurer: Anne Birgitte Gammeljord
Speaker of the Senate: Reinhard Zimmermann
Secretary-General: Vanessa Wilcox

Scientific Director: Christiane Wendehorst

European Law Institute
Schottenring 16/ 175
1010 Vienna
Austria
Tel: + 43 1 4277 22101
Email: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

Approved by the ELI Council on 28 May 2026.

ISBN: 978-3-9505990-3-9
© European Law Institute 2026

Acknowledgement is due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011.

This project is co-funded by
the European Union

Table of Contents

Acknowledgements 6

Executive Summary 7

I. Introduction 9

II. Fraud Prevention and Detection 14

a. Preliminary Remarks 14
b. Early Access to Actionable Information 18
c. National Anti-Fraud Strategies 21
d. Use of AI and Anti-Fraud Tools 21
e. Further Proposals 22
f. Protection of Fundamental Rights 23

III. Improving Investigation and Prosecution Capabilities 24

a. Preliminary Remarks 24
b. Improving Complementarity between EPPO and OLAF Investigations 26
c. Improving Access to and Exchange of Fraud-Related Data 27
d. Leveraging New Technologies and AI 28
e. Effectiveness of Investigation and Prosecution of PIF Crimes 29
f. Ensuring the Protection of Fundamental Rights 33

IV. Making the Recovery Process More Efficient 34

a. Preliminary Remarks 34
b. Protecting the EU Budget through Precautionary and Recovery Measures 34
c. Facilitating Recovery of Assets and Proceeds 35
d. Strengthening Deterrence 36

V. Improving the Governance of the Anti-Fraud Architecture 38

Acknowledgements

Authors
Duarte Nunes (Professor, University of Lisbon)
Ester Herlin-Karnell (Professor, University of Gothenburg)
Robert Kert (Professor, Vienna University of Economics and Business)

Advisor
Valsamis Mitsilegas (Professor, University of Liverpool)

ELI Project Officer
Tomasz Dudek (Senior Project Officer, European Law Institute)

Executive Summary

This European Law Institute (ELI)'s response endorses the European Commission's White Paper for the Anti-fraud Architecture Review.

This response begins with an introduction, which explains that fraud against the European Union (EU)'s financial interests is a form of economic crime, which in many cases is strongly linked to organised crime, terrorism, and cybercrime, causing serious social and economic impacts. In fact, although economic crime, organised crime, terrorism, and cybercrime are distinct criminal phenomena, there are close relationships between them and, moreover, extensive overlapping areas.

Detecting and investigating economic crimes is extremely difficult. These difficulties are even greater in cases where crimes are committed within criminal organisations or terrorist groups. One way to overcome these difficulties is through a proactive response rather than a merely reactive approach.

The first degree of a proactive approach is the so-called situational prevention, that is, a strategy that aims to reduce opportunities for fraud by focusing on manipulating the physical and social environment to make fraud more difficult to commit. Therefore, the procedures for awarding funding or monitoring the implementation of funding programmes must be reviewed and, where necessary, improved, in order to make it as difficult as possible to commit fraud, whether at the stage of awarding the funding or during its implementation. It is also essential to ensure that there are no conflicts of interests, or to minimise the likelihood of their occurrence as much as possible. The same applies to the tax system, in order to prevent or hinder tax evasion. However, this first degree should be complemented with the possibility of conducting preventive investigations. To that aim, some proposals are presented regarding:

(a) How to improve early access to actionable information on reported irregularities and fraud, in order to ensure that all actors take appropriate actions as early as possible at both national and EU level, aiming at enhancing prevention and detection capabilities of fraud throughout the EU;

(b) How can national anti-fraud strategies strengthen the fight against fraud;

(c) How can the use by EU Member States and Anti-fraud Architecture (AFA)'s actors of new Artificial Intelligence (AI) tools, as well as that of existing tools such as the European Early Detection and Exclusion System (EDES) and Arachne+ be leveraged in order to increase the level of prevention/detection;

(d) Adding some new offences to the list of 'Other criminal offences affecting the Union's financial interests'; and

(e) Providing the use in preventive investigations *ante delictum* of the same investigative tools that may be used in criminal prosecution.

Regarding improving investigation and prosecution capabilities, as fraud against the EU's financial interests is a form of economic crime, those who commit such crimes – white-collar criminals – are characterised, amongst other things, by their social influence and by being rational criminals who weigh the advantages and disadvantages of committing crimes against law-abiding conduct. Although in some cases there may be a need to rehabilitate white-collar criminals, the main strategy for combating fraud against the EU's financial interests must be based on deterrence.

Deterrence will tend to be achieved by increasing the risks that criminals face when engaging in fraud, so that the benefits of committing fraud are no longer worth the risk. These risks will be increased if the effectiveness of crime detection, investigation and prosecution is improved and also if offenders can expect the legal consequences of crime (particularly sanctions and confiscation) to be severe. The imposition of severe legal consequences depends on the effectiveness of crime detection, investigation and prosecution. Therefore, some proposals are presented regarding:

(a) How could the criminal investigations conducted by the European Public Prosecutor's Office (EPPO) be complemented, where appropriate, by administrative investigations conducted by the European Anti-Fraud Office (OLAF) in a more effective way, with a view to establishing a solid basis for the early adoption by the Commission of administrative measures, including precautionary and/or recovery measures;

(b) How could access to the relevant data regarding suspicion of fraud or financial crimes affecting the interests of the EU, and timely access and transmission of relevant information between AFA actors, be improved;

(c) How could the use of new technologies and AI to increase the efficiency of AFA actors be leveraged; and

(d) How could the effectiveness of investigation and prosecution of crimes against the financial interests of the European Union (*Protection des Intérêts Financiers* [PIF] crimes) at national and EU level be improved.

Regarding making the recovery process more efficient, in the case of fraud against the EU's financial interests, asset recovery enables the EU to recover both revenue of which it has been unlawfully deprived, and which is necessary for the pursuit of the EU's objectives, and funding that was wrongly granted to fraudsters, allowing it to be used for the purposes intended under that funding programme. Asset recovery also reinforces the deterrent effect of the sanctions imposed on criminals, prevents offenders from benefiting from the proceeds of crime, restores the legal order of assets, and prevents assets obtained through criminal activity from being reinvested in further criminal activities. Because the objectives of asset recovery are not achieved merely by issuing a confiscation order, being necessary to ensure the effectiveness of that order by tracing, seizing and freezing assets, some proposals are presented regarding:

(a) How can recoveries to the EU budget be facilitated, particularly through the transfer of proceeds from insolvency procedures and from seized and confiscated assets following EPPO's investigations, including by leveraging EPPO's role in criminal proceedings to support the recovery of such assets in favour of the Union's budget; and

(b) How can deterrence actions by AFA actors be further strengthened.

Finally, it is emphasised that all these improvements will have to comply with the limitations and safeguards provided in (a) the European Convention on Human Rights (ECHR) (including the case law of the European Court of Human Rights [ECtHR]), (b) EU law, especially the Charter of Fundamental Rights of the European Union and legislation concerning data protection (including the case law of the Court of Justice of the European Union, CJEU), and in (c) the Member States' constitutions.

I. Introduction

The Treaty on the Functioning of the European Union provides that countering fraud and any other illegal activities affecting the EU's financial interests is the shared responsibility of the EU and its Member States[1], **and entrusts the European Commission with a key responsibility to protect the EU's financial interests**[2]. The protection of the Union's financial interests concerns not only the management of budget appropriations, but extends to all measures which negatively affect, or which threaten to negatively affect, its assets and those of the Member States, to the extent that those measures are of relevance to Union policies[3]. Given that the protection of the Union's financial interests requires a common definition of fraud, this task was carried out through the adoption of Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. Articles 3 and 4 of the Directive include the list of criminal offences related to fraud that harms the financial interests of the Union, which comprises offences such as fraudulent conduct with respect to revenues, expenditure and assets at the expense of the general budget of the EU (including financial operations such as borrowing and lending activities), VAT fraud, corruption, and money laundering.

These offences are economic crimes, **which can be defined as acts or omissions classified as crimes by law by one or more individuals possessing knowledge specific to the actors in the political**, **economic**, **commercial**, **or financial world**, **preferentially resorting to corruption and fraudulent methods** – **and**, **if necessary**, **also to violence and intimidation** – **aiming to obtain economic gain**[4].

The impact of economic crime on society is severe: it causes significant financial losses, undermines citizens' trust in democratic institutions, weakens the rule of law, destroys fair competition, discourages investment, destabilises economies, hinders development, exacerbates inequality, and diverts resources away from public services, especially health and education. Direct costs vary and can include lower revenues, higher expenditures, lost banking services, and even increased financial instability. The indirect costs are even greater because they are imposed across an economy, whether by fuelling boom-and-bust cycles or making home prices unaffordable. Potential financial instability impacts include bank runs and lost foreign investment. Large-scale money laundering can even spur volatility in international capital flows, undermine good governance, spark political instability, and generally erode trust in governments and institutions[5]. In short, although economic crimes are usually mentioned as examples of victimless crimes, in reality, economic crime is not a victimless crime.

Although economic crime, **organised crime**, **terrorism**, **and cybercrime are distinct criminal phenomena**, **there are close relationships between them and**, **moreover**, **extensive overlapping areas**. Furthermore, authorities are not dealing with two separate criminal worlds, one inhabited by dangerous criminals smuggling drugs, or trafficking people, and the other supposedly less dangerous white-collar criminals, 'merely' corrupting and laundering money. These words go hand in hand. They grow together. As long as people do not understand this fundamental link, authorities will not be able to stop the growth and expansion of serious organised crime groups[6].

---

[1] See Articles 310(6) and 325 TFEU.

[2] See Article 317 TFEU.

[3] See Recital 1 of Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law.

[4] See Duarte Rodrigues Nunes, *O problema da admissibilidade dos métodos 'ocultos' de investigação criminal como instrumento de resposta à criminalidade organizada*, Gestlegal, Coimbra, 2019, p 143.

[5] See Carolina Claver, Chady El Khoury, Rhoda Weeks-Brown, *Financial Crimes Hurt Economies and Must be Better Understood and Curbed*, IMF Blog, December 7, 2023, https://www.imf.org/en/blogs/articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed.

[6] EPPO, *Annual Report 2023*, https://www.eppo.europa.eu/assets/annual-report-2023/pdfs/EPPO_Annual_Report_2023_en.pdf , p 5.

Regarding the relationship between economic crime, organised crime and terrorism, firstly, both criminal organisations and terrorist groups engage in money laundering activities, in order to disguise the origins of their assets obtained from criminal activities, as a way to avoid confiscation and conceal evidence of those criminal activities[7].

In the case of fraud against the EU's financial interests, it has been noted that even when fraud is limited to a single country, criminal networks have created structures in other countries to conceal their criminal activities and launder proceeds. In some cases, they have reproduced the same fraudulent schemes across multiple Member States, thereby underlining the ever-present international dimension of organised crime[8].

Secondly, **corruption is essential for criminal organisations and terrorist groups**, whether to pursue a 'specific' objective (especially when operating within the legitimate economy, eg to obtain the public contracts or funding) or to protect the organisation from the authorities[9]. As mentioned in the White Paper for the Anti-fraud Architecture Review, corruption constitutes a particularly serious threat to the Union's financial interests, which can, in many cases, also be linked to fraudulent conduct. In reality, the Union's financial interests can be negatively affected by certain types of conduct (especially corruption) of a public official who is entrusted with the management of funds or assets, whether they are in charge of managing the funds, or act in a supervisory capacity.[10]

Thirdly, **both criminal organisations and terrorist groups are increasingly intervening in the legitimate economy**, **and currently**, **this is a very substantial part of their activities**, and not something merely incidental to illicit activities. This intervention in the legitimate economy pursues a fourfold purpose: to obtain economic gain (including for the financing of terrorism); to protect the organisation, its members, and its assets from the authorities (through money laundering or creating a front for illicit activities); the establishment of relationships with members of the world of politics, business, institutions, and public administration; and to obtain social consensus among the populations of the regions where these organisations and groups operate.

Given that criminal organisations and terrorist groups do not accept the 'business risk', they will use illicit methods to ensure profit and to drive rival companies out of the market. These methods can include acts of violence and intimidation as well as economic crimes (corruption, money laundering, tax crimes, fraud in obtaining funding, environmental crimes, etc)[11].

Regarding fraud against the EU's financial interests, **in some cases**, **perpetrators create companies** (**including shell companies**) **or take over inactive ones**, **in order to fraudulently obtain funding and/or apply for funds**. In cases related to R**ecovery and Resilience Facility** (RRF) funds, the companies do not have physical offices and had not submitted the required tax returns, some for more than 20 years. In many cases, perpetrators create, with the help of accountants, a paper trail showing revenues in millions, allowing them to submit multiple requests for funding. They also create a 'carousel' of 'letterbox companies' to produce millions in illicit revenues. In many cases, funding is immediately diverted from the companies' bank accounts, through systematic cash withdrawals from ATMs, or bank transfers to the accounts of other individuals or companies. Organised crime involvement is apparent every time the fraudulent scheme is set up on a large-scale and ensures high-value illicit profit. In these cases, criminal groups coordinate several small companies under a multi-territory fraud scheme involving sham entities,

---

[7] See Duarte Rodrigues Nunes, *O problema da admissibilidade dos métodos 'ocultos' de investigação criminal como instrumento de resposta à criminalidade organizada*, cited above, p. 126-128 and 181.

[8] EPPO, *Annual Report 2025*, https://www.eppo.europa.eu/assets/annual-report-2025/pdfs/EPPO_Annual_Report_2025_en.pdf, p 72.

[9] See Duarte Rodrigues Nunes (n 4) p 120-122 and 181.

[10] See Recitals 8 and 9 of Directive (EU) 2017/1371, cited above.

[11] See Duarte Rodrigues Nunes, 'Criminalidade organizada e economia lícita: *Intimidazione del vincolo associativo* ou *Joint Venture*?', *Criminalidade Organizada Transnacional*, *Corpus Declicti – III*, Almedina, Coimbra, 2021, p 46-52.

professional enablers, and laundering strategies with a final destination in third countries, including offshore havens[12].

Fourthly, **there is the so-called economic organised crime**, which can be defined as acts or omissions classified as crimes by law by a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more crimes, whose members are endowed with knowledge specific to the actors in the world of politics, business, institutions, and public administration, acting within the scope of their professional activity, preferably resorting to corruption and fraudulent methods (and, if necessary, to violence and intimidation), aiming to obtain economic gain and to protect the criminal group and its members from criminal prosecution.

There are essentially three forms of organised economic crime: (**1**) **economic crimes committed by 'traditional' organised crime or terrorist groups infiltrating the legitimate economy**; (**2**) **white-collar criminals who associate to commit economic crimes using the world of politics**, **business**, **institutions**, **or public administration**; **or** (**3**) **legitimate corporations that commit economic crimes systematically**[13].

As mentioned in the White Paper for the Anti-fraud Architecture Review, **there is growing evidence of organised crime playing a key role in fraud schemes against the EU's financial interests**, **and**, **conversely**, **of the important role of fraud in financing other forms of serious and organised crime**, **including terrorism**[14]. Consequently, if terrorist groups and organised violent crime groups (far-left extremists, far-right extremists, or otherwise) also finance themselves through fraud, then, preventing and combating fraud against the financial interests of the Union contributes indirectly to preventing terrorism and other forms of organised violent crime.

Fraud against the financial interests of the Union is aimed at obtaining financial gains, but criminal and terrorist organisations may pursue other aims, such as money laundering. One method of money laundering is to take out unnecessary bank loans: criminals obtain money with an undoubtedly legitimate origin and then repay the loan with money of illicit origin. Financial support from the EU can be used for the same purpose. In the case of criminal organisations and terrorist groups, these types of fraud also serve another purpose, which can be described as strategic. Criminal organisations and terrorist groups take advantage of poor socio-economic conditions of the populations in the regions where they operate. Thus, they have a strong interest in preventing improvements in the living conditions of the inhabitants of the regions where they operate, as it would jeopardise the recruitment of new members. Therefore, when committing fraud in cases where the assets appropriated by organised crime are intended to improve the living conditions of the inhabitants of those regions, criminal organisations and terrorist group are not only obtaining financial gain, but also securing their sources for recruiting new members[15].

Regarding the relationship between economic and cybercrime[16], **white-collar criminals plan**, **commit**, **and/or conceal traces of their crimes** (**including through money laundering**), **taking advantage of the benefits offered by the use of computer technology to hinder the detection of crimes and the collection of evidence**[17]. In this particular scenario, as mentioned in the White Paper for the Anti-fraud Architecture Review, fraudsters now make

---

[12] See EPPO, *Annual Report 2024*, https://www.eppo.europa.eu/assets/annual-report-2024/pdfs/EPPO_Annual_Report_2024_en.pdf, p 71.

[13] See Duarte Rodrigues Nunes (n 4) p 152-156, and Andrea Di Nicola, *La criminalità economica organizzata*, *Le dinamiche dei fenomeni*, *una nuova categoria concettuale e le sue implicazioni di policy*, Franco Angeli, Milan, 2006, p 86-89.

[14] See Recital 7 of Directive (EU) 2017/1371, cited above. See also EPPO, *Annual Report 2023*, https://www.eppo.europa.eu/assets/annual-report-2023/pdfs/EPPO_Annual_Report_2023_en.pdf, p. 4,

[15] See Duarte Rodrigues Nunes (n 4) p 18 (footnote 5), and Pietro Grasso/Alberto La Volpe, *Per Non Morire di Mafia*, Sperling&Kupfer, Milan, 2009, p 265-267.

[16] Concerning the relationship between economic crime and cybercrime, see Duarte Rodrigues Nunes, *Os crimes previstos na Lei do Cibercrime*, *2.ª Edição*, Gestlegal, Coimbra, 2024, p 38-39.

[17] Concerning the reasons why criminals use computer technology to commit crimes, see Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, *2.ª Edição*, Gestlegal, Coimbra, 2021, p 18-25.

use of advanced technologies like AI, encrypted communications, and crypto currencies, to carry out, and hide, their criminal activities.

For all these reasons, the effectiveness of preventing and combating fraud against the financial interests of the Union depends on a comprehensive approach that takes into account the relationships between fraud against the financial interests of the Union, on the one hand, and the actions of criminal organisations and terrorist groups, other forms of economic crime (including corruption and money laundering), and cybercrime, on the other hand.

Detecting and investigating economic crimes is extremely difficult[18]. However, **when economic crimes are committed within criminal organisations or terrorist groups**, **difficulties inherent in investigating organised crime or terrorism**[19] **are added to those present in investigating economic crime**. One way to overcome these difficulties is through a proactive response rather than a merely reactive approach (ie after the authorities become aware of the crime). **Although proactive investigation** (**crime prevention**, **preventive investigations *ante delictum***) **and reactive investigation** (**criminal prosecution**) **are distinct realities**, **the dogmatic difference that has always existed between them has become blurred due to the fact that the actions of authorities in responding to organised crime**, **terrorism and even economic crime have shifted to the** '**forward field**' **and that investigative methods normally used in criminal proceedings are increasingly employed in preventive investigations *ante delictum***. **Today**, **there is a *continuum* between crime prevention and criminal prosecution in matters regarding the responses to organised crime and terrorism**, **with proposals for the creation of intermediate legal instruments such as forward field investigations** (**which are subsequently divided into** '**measures for the future prosecution of crimes**' **and** '**preventive combat against crime**')[20]. **The same approach can be used against economic crime**. **Proactive investigation aims at obtaining *notitia criminis***, **and/or information that facilitates the investigation of crimes that may be committed or relates to the *modus operandi* of certain types of criminality and its change**, **and/or to prevent the commission of already planned crimes or minimise their effects on victims**[21].

Given that white-collar criminals tend to be rational criminals who weigh the advantages and disadvantages of committing crimes against law-abiding conduct, **both applicable and applied sanctions must be sufficiently deterrent**[22]. **At the level of the legal consequences of crime**, **the confiscation of the proceeds of crime is essential**, **not only because it prevents criminals from enjoying or reinvesting these proceeds in the commission of new crimes**, **but also because**, **indirectly**, **it can deter the commission of crimes**, **especially in the case of the confiscation of unexplained wealth with a reversal of the burden of proof**[23].

In fact, EPPO's investigations demonstrate that **criminal enterprises operating in the field of VAT and customs fraud achieve very high profits while facing relatively low risks**. This explains why conventional criminal activities focusing on illegal goods (counterfeited goods, currency counterfeiting, drugs, substandard goods, weapons, etc), or on criminal exploitation of vulnerable

---

[18] Regarding the reasons why detecting and investigating economic crimes is extremely difficult, see Duarte Rodrigues Nunes (n 4) p 149-151 and 348, Laura Zuñiga Rodríguez, 'Criminalidad de Empresa, Criminalidad Organizada y Modelos de Imputación Penal', *Delincuencia Organizada*, *Aspectos penales*, *procesales y criminológicos*, Universidad de Huelva Publicaciones, Huelva, 1999, p 206-210, and Ruggiero, *Organized and Corporate Crime in Europe*, *Offers that Can´t Be Refused*, Dartmouth, Aldershot, Brookfield, Singapore and Sydney, 199, p 8-9.

[19] Concerning the reasons why the investigation of organised crime and terrorism is so difficult, see Duarte Rodrigues Nunes (n 4) p 342-348.

[20] ibid p 255-256.

[21] Ibid p 257.

[22] See Duarte Rodrigues Nunes, *Curso de Direito Penal*, *Parte Geral*, *Tomo II*, *Questões fundamentais*, *Consequências Jurídicas do Crime*, Gestlegal, Coimbra, 2025, p. 502-503. See also EPPO, *Annual Report 2023*, https://www.eppo.europa.eu/assets/annual-report-2023/pdfs/EPPO_Annual_Report_2023_en.pdf, p 4.

[23] See Duarte Rodrigues Nunes, *Lei de combate à criminalidade organizada e económico-financeira comentada e anotada com a Jurisprudência*, Gestlegal, Coimbra, 2025, p. 112-113.

people (exploitation of labour, prostitution, human trafficking) are increasingly combined with criminal activities related to the trading of legal goods, carried out using criminal modalities that cause massive damage to the financial interests of both the EU and its Member States. These activities remain difficult to detect from a purely national perspective[24].

It is important to bear in mind that fraud against the Union's financial interests involves not only those who will benefit from the funding, but also political decision-makers who grant it, the officials who participate in the funding allocation procedures, and the professionals who sell their services to the fraudsters[25]. Regarding money laundering, the role of professional money launderers is crucial. Professional money launderers have established underground financial systems to process transactions quickly and efficiently, providing their services to any organised crime group, regardless of the predicate offences, or territorial operational area[26]. Therefore, measures to prevent and combat fraud will have to be more comprehensive, in order to include all these actors.

Any proposal to improve the 'EU anti-fraud architecture' should therefore answer a difficult yet very important question: how is it possible that organised crime groups were, and still are, able to develop VAT fraud to an industrial level, despite all the anti-fraud strategies, auditing and reporting[27]?

However, there is also the other side of the coin: the side of fundamental rights of citizens, including those that are suspected of being involved in crime. Therefore, all these instruments for preventing and combating fraud against the EU's financial interests must respect the limitations and safeguards provided in (a) the ECHR (including the case law of the ECtHR), (b) in EU law, especially the Charter of Fundamental Rights of the European Union and legislation concerning data protection (including the case law of the CJEU), and (c) in the domestic law of the Member States.

---

[24] EPPO, *Annual Report 2025*, https://www.eppo.europa.eu/assets/annual-report-2025/pdfs/EPPO_Annual_Report_2025_en.pdf, p 72.
[25] See EPPO, *Annual Report 2024*, https://www.eppo.europa.eu/assets/annual-report-2024/pdfs/EPPO_Annual_Report_2024_en.pdf, p 70-71.
[26] Ibid p 70.
[27] ibid p 5.

II. Fraud Prevention and Detection

a. Preliminary Remarks

Fraud against the EU's financial interests causes damage to the EU's assets through the unauthorised access to, or misuse of, funds from funding programmes. It also causes harm to those who submit applications for other projects that are genuinely deserving of funding and support. However, in addition to this more direct harm, there are other collateral effects of fraud, such as the undermining of a programme's objectives, the loss of credibility and trust in the bodies that operate it and, ultimately, in the EU itself and its institutions.

As mentioned above, detecting and investigating economic crime is extremely difficult, and one way to overcome these difficulties is through a proactive response rather than a merely reactive approach.

The first degree of a proactive approach is situational prevention, that is a strategy that aims to reduce opportunities for fraud by focusing on manipulating the physical and social environment to make fraud more difficult to commit. Therefore, the procedures for awarding funding or monitoring the implementation of funding programmes must be reviewed and, where necessary, improved, in order to make it as difficult as possible to commit fraud, whether at the stage of awarding the funding or during its implementation. **It is also essential to ensure that there are no conflicts of interest, or to minimise the likelihood of their occurrence as much as possible. The same applies to the tax system, in order to prevent or hinder tax evasion.**

As mentioned in the White Paper for the Anti-fraud Architecture Review, the 2024 Financial Regulation[28] has introduced several innovations that will help further strengthen the prevention, detection, correction and follow-up of irregularities, including fraud and corruption from the next Multiannual Financial Framework (MFF) onward. They include:

(a) several improvements to the EDES[29] and the extension of its scope to shared management (and to direct management with the Member States) as from 1 January 2028. The EDES allows fraudulent or unreliable economic operators to be detected at an early stage and based on alleged facts. If misconduct is established, an economic operator can be temporarily excluded from receiving EU funds for up to five years. EDES cases can also, in certain conditions, lead to the imposition of financial penalties. Decisions are registered in a central database that can be accessed by all Institutions, Bodies, Offices, and Agencies (IBOAs) and Member State authorities;

(b) the compulsory feeding of the single data mining and risk-scoring tool (Arachne+) for audit and control purposes as from 1 January 2028. Data collected by all Member States' authorities as regards all funds will be included in a single EU-wide tool. This will enhance control and audit functions across the EU and assist national authorities and AFA actors in the prevention, detection, correction and follow-up of fraud, corruption and irregularities, including conflicts of interest and double-funding. The use of Arachne+ by managing authorities will remain voluntary, but the European Parliament, the Council and the Commission have agreed to re-examine the compulsory use of Arachne+ based

[28] Regulation 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast).

[29] The EDES was set up in 2016 as one of the instruments to protect the EU's financial interests.

on an assessment of the readiness of the tool to be delivered by the Commission in 2027[30].

The 2024 Financial Regulation provides, among other aspects, standardised measures to collect, compare and aggregate information on recipients of Union funds, including identifying the natural persons that ultimately benefit, directly or indirectly, from Union funding or the misuse of that funding.

The electronic recording and storage of data on recipients of Union funds, including their beneficial owners as defined in Article 3 (6) of Directive (EU) 2015/849 of the European Parliament and of the Council, and the regular making of those data available in a single integrated and interoperable information and monitoring system, including a single data mining and risk-scoring tool (single integrated IT system), should facilitate risk assessment for the purposes of selection, awarding, financial management, monitoring, investigation, control and audit and contribute to effective prevention, detection, correction and follow-up of irregularities including fraud, corruption, conflicts of interest and double-funding[31].

Article 36 (2) (d) of Regulation 2024/2509 specifically provides that for the purposes of budget implementation, internal control shall be applied at all levels of management and shall be designed to provide reasonable assurance for prevention, detection, correction and follow-up of irregularities including fraud, corruption, conflicts of interest and double-funding, also through the voluntary use of a single integrated and interoperable information and monitoring system, including a single data mining and risk-scoring tool, provided by the Commission, and allowing for the access to, and the electronic automatic retrieval, recording, storage and analysis of, data on the recipients of Union funds including their beneficial owners, as defined in Article 3 (6) of Directive (EU) 2015/849, in accordance with sector-specific rules.

The 2024 Financial Regulation also provides conditions and procedures for suspending, terminating or reducing a Union contribution in the case of beneficiaries who are not suitable to apply for or to be selected for implementing Union funds, or to receive such funds under a programme in shared management[32].

Finally, in order to improve the prevention of fraud against the EU's financial interests, as mentioned above, the 2024 Financial Regulation provides several improvements to the EDES, such as an expedited procedure, a legal presumption of notification, the possibility of excluding beneficial owners, and a few new cases of grave professional misconduct that can lead to exclusion[33]. The 2024 Financial Regulation should facilitate the identification of natural persons who benefit from Union funding. To prevent the use of shell companies, these data **should be automatically verifiable against the formal ownership and encumbrance information held in Land and Mercantile Registries**.

As also mentioned above, although proactive investigation (crime prevention) and reactive investigation (criminal prosecution) are distinct realities, the dogmatic difference that has always existed between them has become blurred due to the fact that the actions of authorities in responding to organised crime, terrorism and even economic crime have shifted to the 'forward field' and that investigative methods normally used in criminal proceedings are increasingly employed in preventive investigations *ante delictum*. Therefore, there will have to be a *continuum* between crime prevention and criminal repression when responding to fraud against the EU's financial interests.

---

[30] See European Commission, *White Paper for the Anti-fraud Architecture Review*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0546&qid=1753799750304, pp 6-7.

[31] See Recital 29 of Regulation 2024/2509, cited above.

[32] See Articles 137 to 144, and Recitals 105-116.

[33] See White Paper for the Anti-fraud Architecture Review, p 7 (footnote 31).

According to the EU Anti-fraud Architecture, while OLAF is responsible for carrying out administrative investigations to protect the EU's financial interests against fraud, corruption and any other illegal activity, and is the Commission's lead service in the conception and development of a European anti-fraud policy, EPPO is responsible for investigating, prosecuting and bringing to court perpetrators of criminal offences that affect the EU's financial interests as set out in the PIF Directive[34] ('PIF offences'), including fraud, corruption and money laundering, as well as organised crime when the focus is on PIF offences, in accordance with the EPPO Regulation[35].

When OLAF concludes an investigation, it often issues recommendations to the competent EU and national authorities, inviting them to take action to redress the fraud, corruption or other illegal activity uncovered by the investigation. OLAF's recommendations are intended to protect the EU budget and to uphold the rule of law. More specifically, OLAF's recommendations aim to serve several purposes:

(a) Financial recommendations: OLAF invites competent EU or national authorities to recover amounts that were unduly spent or prevent them from being irregularly spent, or in customs matters, not duly collected for the EU budget as a result of fraud or irregularities;

(b) Judicial recommendations: OLAF invites the competent authorities to consider initiating criminal proceedings;

(c) Disciplinary recommendations aim to sanction wrongdoing by EU staff or members of EU bodies; and

(d) Administrative recommendations aim to reinforce existing policies and control systems. OLAF can also recommend a specific administrative action, such as excluding an entity from future EU funding or to perform an audit or an administrative check. Administrative recommendations can also address systemic weaknesses uncovered in control systems.

However, despite the close cooperation between OLAF and EPPO as provided in Regulation (EU) 2017/1939, Regulation (EU, Euratom) No 883/201, and in the working arrangement between EPPO and OLAF[36], OLAF's investigations serve purely administrative purposes and are not aimed at preventing crime. Consequently, OLAF's investigations can only indirectly contribute to crime prevention. In any case, OLAF does not currently have the authority to carry out preliminary investigations for the purposes of crime prevention.

For its part, the objective of the recently created Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)[37] is to protect the public interest, the stability and integrity of the Union's financial system, and the proper functioning of the internal market by:

(a) preventing the use of the Union's financial system for the purposes of money laundering and terrorist financing (ML/TF);

(b) contributing to the identification and assessment of ML/TF risks and threats across the internal market, as well as risks and threats originating from outside the Union that impact, or have the potential to impact, the internal market;

---

[34] Directive (EU) 2017/1371, cited above.

[35] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO').

[36] OLAF and EPPO have signed the Working Arrangement between the European Anti-Fraud Office and the European Public Prosecutor's Office, 5 July 2021, https://www.eppo.europa.eu/sites/default/files/2021-07/Working_arrangement_EPPO_OLAF.pdf.

[37] AMLA was created by Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. Its purpose is to prevent money laundering and the financing of terrorism. It will be fully operational as from 1 January 2028. Its powers will enable it to support the operational coordination of national authorities tasked with supervision or with producing financial intelligence. In addition, AMLA has been conferred direct supervisory powers, including the possibility to impose pecuniary sanctions and administrative measures on operators and financial institutions (including banks) under its direct supervision, to ensure that they correctly and consistently apply the EU rules on anti-money laundering and on countering the financing of terrorism. These rules have been overhauled and will apply across the EU as of mid-2027.

(c) ensuring high-quality supervision in the area of anti-money laundering and countering the financing of terrorism (AML/CFT) across the internal market;

(d) contributing to supervisory convergence in the area of AML/CFT across the internal market;

(e) contributing to the harmonisation of practices in the detection of suspicious transactions or activities by Financial Intelligence Units (FIUs); and

(f) supporting and coordinating the exchange of information between FIUs, and between FIUs and other competent authorities[38].

AMLA has supervisory and investigative powers as stated in Articles 17 to 21 and the power to impose pecuniary sanctions and periodic penalty payments as provided for in Articles 22 and 23 of Regulation (EU) 2024/1620- It also has the powers and obligations which financial supervisors have in the area of AML/CFT under the applicable Union law, unless otherwise provided for by Regulation (EU) 2024/1620[39]. In addition, AMLA has powers to support and coordinate FIUs in matters of anti-money laundering and countering the financing of terrorism. In light of the cross-border nature of ML/TF, effective and efficient cooperation, information exchange and coordinated action between FIUs are of crucial importance, in order to improve such coordination and cooperation, AMLA is empowered to support and coordinate the activities of FIUs. AMLA must be informed of any disagreements between FIUs in relation to cooperation matters and the exchange of information, and is able to act as a mediator between the relevant FIUs[40]. AMLA has the authority to propose, initiate, coordinate and support, with all appropriate means, joint analyses of suspicious cross-border transactions or activities. A joint analysis is to be triggered where there is a need for one pursuant to the relevant provisions of EU law and in accordance with the methods and criteria for the selection and prioritisation of cases relevant for the conduct of joint analyses developed by AMLA[41]. AMLA can also request FIUs to initiate a joint analysis under specific circumstances, including where information has been brought to its attention by whistleblowers or investigative journalists or where the joint analysis of complex and cross-border cases would add value[42].

Identifying, at an early stage, links with information held by other EU's bodies, offices and agencies and by relevant third parties is critical to ensure that the most relevant cross-border cases, including those requiring extensive operational analysis, are selected[43]. Therefore, AMLA, EPPO, European Union Agency for Law Enforcement Cooperation (Europol), European Union Agency for Criminal Justice Cooperation (Eurojust) and OLAF may exchange strategic and other non-operational information, such as typologies and risk indicators, in the areas within their competence[44].

Effective operational cooperation in cross-border cases between AMLA and other relevant EU bodies, offices and agencies is of crucial importance. In order to ensure that, where relevant, the results of joint analyses of cross-border cases are followed up effectively, AMLA will transmit the results of joint analyses to EPPO or to OLAF where the results of a joint analysis indicate a criminal offence, in respect of which EPPO or OLAF can exercise their respective competences. Furthermore, subject to the agreement of all FIUs participating in a joint analysis, AMLA will transmit the results of that joint analysis to Europol and Eurojust where the results of that joint analysis indicate that a criminal offence may have been committed in respect of which Europol and Eurojust can exercise their powers[45].

---

[38] See Article 1(3) of Regulation (EU) 2024/1620, cited above.
[39] See Article 6 of Regulation (EU) 2024/1620, cited above.
[40] See Article 39(3)(2) of Regulation (EU) 2024/1620, cited above.
[41] See Article 40 of Regulation (EU) 2024/1620, cited above.
[42] See Article 42 of Regulation (EU) 2024/1620, cited above.
[43] See Recital 45 of Regulation (EU) 2024/1620, cited above.
[44] See Article 41(6) of Regulation (EU) 2024/1620, cited above.
[45] See Article 41 of Regulation (EU) 2024/1620, cited above.

It would therefore be useful to provide EPPO with the possibility to carry out preventive investigations *ante delictum*, with the assistance of Europol and – in the case of money laundering and financing of terrorism – AMLA. Assigning these powers to EPPO rather than to another body (eg OLAF) would have the advantage of centralising the powers for the prevention and criminal prosecution of fraud against the EU's financial interests, and other criminal offences affecting the Union's financial interests within a single body: as mentioned above, there needs to be a *continuum* between prevention and criminal prosecution in order to ensure a more effective response to economic crime.

As stated above, there is growing involvement of criminal organisations and terrorist groups in fraud against the EU's financial interests.

Therefore, the effective prevention of fraud against the EU's financial interests is also essential to preventing and prosecuting organised crime and terrorism. Thus, it would be useful to provide the possibility of applying, in preventive investigations *ante delictum*, investigative means that are used in criminal proceedings in order to make the prevention of fraud against the EU's financial interests more effective and, at the same time, to improve the prevention and suppression of organised crime and terrorism.

Naturally, all these changes will have to comply with the limitations and safeguards provided in (a) the ECHR (including the case law of the ECtHR), and in (b) EU law, especially the Charter of Fundamental Rights of the European Union and legislation concerning data protection (including the case law of the CJEU), and (c) in the domestic law of the Member States.

b. Early Access to Actionable Information

In accordance with the law in force, where OLAF suspects criminal conduct, it is required to submit a report to EPPO without undue delay. The objective of the 'hit/no-hit' procedure is to ensure that OLAF does not open an investigation where EPPO has already opened one on the same facts, and to determine the competence for an investigation. According to the working arrangements in place, the hit/no-hit starts with OLAF consulting EPPO on whether EPPO is investigating certain persons or projects. Where EPPO is not investigating these persons or projects, OLAF, in the absence of suspicion of criminal conduct, may decide to proceed with its own investigation. A positive hit will give rise to a series of consultations where both parties try to ascertain whether the facts are the same. If EPPO confirms that the facts are not the same, OLAF may open an investigation. For positive hits, if EPPO does not object to OLAF's specific reasoned request, OLAF may open a parallel complementary investigation to EPPO, with a view to taking administrative action. During such complementary investigations, OLAF must remain in regular consultation with EPPO.

The European Court of Auditors (ECA) recommended that the Commission, in collaboration with EPPO, should establish an interoperable anti-fraud system, in full compliance with the relevant legal framework, data protection rules and the need for confidentiality in criminal investigations. The system should make it clear where allegations of fraud should be reported, and facilitate an efficient exchange of information on fraud allegations and investigations. Within this framework, the new system should be based on the following principles[46]:

(a) all allegations received are channelled to a central repository with a view to establishing an efficient process for their assessment;

[46] See European Court of Auditors, *Special report 26/2025: EU bodies fighting fraud – Clear mandates but exchange of information and Commission oversight remain insufficient*, https://www.eca.europa.eu/ECAPublications/SR-2025-26/SR-2025-26_EN.pdf.

(b) fraud allegations originated by OLAF, and ongoing OLAF investigations that uncover suspicions of criminal conduct, are referred to EPPO without undue delay, or, where EPPO is not competent, to the competent national prosecuting office;

(c) in the course of its investigations, as soon as EPPO considers that an allegation is not of a criminal nature, key information is made available to OLAF or, when applicable, to other administrative bodies, and copied to the Commission, to determine whether it would be cost effective to open an administrative investigation; and

(d) during EPPO investigations, EPPO periodically assesses at what point access to relevant information may be granted to the Commission, to determine the scope for administrative action, and to OLAF, to determine whether it would be cost effective for OLAF to propose a complementary investigation.

With regard to point (a), in the interest of preserving the confidentiality of criminal investigations (which is essential to the success of investigations into fraud against the EU's financial interests) and the rights of suspects, such central repository should be managed by EPPO. Therefore, whenever an allegation is qualified from the very beginning as amounting to a PIF crime, EPPO will have access to it immediately, without any further assessment by any other body.

In any case, EPPO must inform the competent body without undue delay, providing it with the information necessary to enable the implementation of administrative measures aimed at preventing or minimising the effects of fraud (eg exclusion from receiving EU funds, suspension of the transfer of further funding instalments, etc).

As mentioned in the White Paper for the Anti-fraud Architecture Review, OLAF has gained considerable experience and developed an extensive network of contact points with Member States and third countries, developing anti-fraud strategies in Member States and non-EU countries. It is therefore proposed that:

(a) OLAF's invaluable expertise in fraud and corruption prevention should be available to all AFA actors to the maximum possible extent;

(b) AFA actors should also be encouraged to use the anti-fraud coordination services (AFCOS), which are coordinated by OLAF, to bolster collaboration between national and EU-level bodies in fraud and corruption prevention; and

(c) Information exchange under Council Regulation (EC) No 515/97 should also be better used to enhance mutual assistance between national administrative authorities in the context of fraud prevention[47].

However, **due to social**, **economic**, **cultural or legislative factors**, **as well as the way in which the authorities operate**, **among others**, **each country has its own peculiarities in terms of fraud**[48], **therefore it is extremely important that both the competent authorities of the Member States and AFA actors are aware of the *modi operandi* of fraudsters operating within Member States or even in non-EU countries**, **if engaging in conduct likely to harm the EU's financial interests**. **In addition**, **in each Member State**, **fraud against the EU's financial interests may be committed either by individuals from that Member State or by individuals from another Member State or from non-EU countries**.

Therefore, in order to acquire comprehensive knowledge about the patterns of fraud across the EU and facilitate prevention and the early detection

[47] Council Regulation No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.

[48] All types of fraudulent conduct, even if not related to fraud against the EU's financial interests, should be reported for inclusion in the database, as such methods can also be used to defraud the EU's financial interests.

of fraud, **it would be useful to create a shared database that is directly accessible both to AFA actors and to the Member States' authorities responsible for preventing and combating fraud against the EU's financial interests**, **and other criminal offences affecting the Union's financial interests** (corruption, money laundering and misappropriation, as well as others that should be added to the list of 'other criminal offences affecting the Union's financial interests', as proposed below).

The effectiveness of fraud prevention and early detection, as well as the adoption of measures designed to fulfil these purposes, will be greater if the authorities can access this information in real time rather than having to request it from another authority, however efficient that procedure may be. This database would include data provided by Member States' authorities, AFA actors, other EU bodies, and eventually authorities of non-EU Member States and/or international organisations, whilst avoiding duplication of data as far as possible. Such data may be data obtained by the authorities of the Member States or the EU (including non-criminal courts and administrative authorities) either directly or indirectly (eg data that has been made available by credible private entities or by the judicial or administrative authorities of non-EU Member States in the context of international cooperation). However, insofar as the data contained in that database may include personal data, this database must comply with the requirements laid down in data protection legislation, in particular the General Data Protection Regulation (GDPR)[49].

Although it can be accessed directly by both AFA actors and Member States' authorities responsible for preventing and combating fraud against the EU's financial interests, and other criminal offences affecting the Union's financial interests, given that it is primarily aimed at preventing and detecting fraud against the EU's financial interests, this database should be managed by EPPO.

As mentioned above, the 2024 Financial Regulation provides conditions and procedures for suspending, terminating or reducing a Union contribution in the case of beneficiaries who are not suitable to apply for or to be selected for implementing Union funds, or to receive such funds under a programme in shared management.

One of these measures is the exclusion of persons or entities referred to in Article 137(2) of the 2024 Financial Regulation, which are to be excluded in accordance with the provisions of Article 138(1). However, **it will be very easy for such individuals or entities to circumvent this exclusion by using front person or front or shell companies**: **indeed**, **in the case of criminal organisations**, **it is very common for them to use reputable companies** (**over which they have gained control**, **eg by providing financial assistance**) **as front companies and their owners and directors as front persons**. Therefore, once a decision regarding exclusion has been made, **it will be important to gather information about other persons** (**family members**, **intimate partners**, **close friends**, **etc**) **or entities within the immediate circle of the excluded person or entity who may be used as front person or front companies**. This information would be gathered by OLAF and should be entered into the aforementioned database (which would facilitate the cross-referencing of data) or into another database.

Another important issue concerns the collection of data on administrative proceedings conducted by the authorities of Member States intended to allocate EU programme funds, including the excessive bureaucracy, which tends to hinder access to funding for certain individuals or entities (particularly smaller businesses) whilst benefiting others (particularly large companies and economic groups). Excessive bureaucracy may result from a lack of competence in defining the criteria for the granting of financing, but it may also be a ploy aimed to favour certain applicants.

It is also important to **gather information on the natural and/or legal persons to whom Member States typically award grants under EU support programmes**, **the date of creation of those legal**

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

persons in relation to the date on which the public competition is launched[50], **the links between those natural persons and/or the owners and directors of those legal entities and the political party to which the government awarding the grant belongs** (**eg whether they are**, **or have been**, **members**, **whether they are**, **or have been**, **donors**, **whether they have held any political office**, **etc**), **or with persons who are**, **or were**, **members of that party**.

If this information is not included in EDES or in Arachne+, in order to facilitate the early detection of signs of fraud – which often requires the analysis of a very large volume of data – it would be useful for both EU and Member States' authorities to have access to advanced analytics tools using AI, machine learning, and complex modelling to uncover hidden patterns and provide predictive insights that are capable of detecting and analysing digital data that may be relevant to the detection of signs of fraud and to the subsequent establishment of the commission of offences.

Naturally, all these improvements will have to comply with the relevant legal framework concerning data protection.

Unjustified failures to take measures, to provide information to the database or to cooperate should result in EU officials being held liable. In the case of Member States' authorities, the Member State concerned should be held liable; the same should apply to the individual liability of officials of the Member State who are responsible for providing such information.

c. National Anti-Fraud Strategies

The authorities of the Member States are the first line of defence in the fight against fraud affecting the EU's financial interests. Thus, as mentioned in the White Paper for the Anti-fraud Architecture Review, in order to further enhance prevention, anti-fraud strategies with related action plans could also be put in place at the national level. However, not all Member States have national anti-fraud strategies and the existing strategies do not necessarily follow a consistent approach, which can lead to weaknesses and gaps in the global anti-fraud approach. Therefore, in order to follow a consistent approach, **it is recommended to establish uniform criteria for the formulation of national anti-fraud strategies**, **while ensuring that national strategies are adjusted to the specific characteristics of fraud in each Member State**. At the same time, the effectiveness of national strategies can be improved in the same terms as described above regarding EPPO.

In addition, it is recommended to provide in the law for obligations on national authorities to report immediately to EPPO any signs of fraud against the EU's financial interests which they become aware of in the course of their duties.

d. Use of AI and Anti-Fraud Tools

As mentioned above, **the detection of signs of fraud often requires the analysis of a very large volume of data**. This data may consist of information already held by the authorities or data that is freely available on the internet. Therefore, **the use by both EU and Member States' authorities of advanced analytics tools using AI**, **machine learning**, **and complex modelling to uncover hidden information and provide predictive insights that are capable of detecting and analysing digital data that may be relevant to the detection of signs of fraud and to the subsequent establishment of the commission of offences is essential both for the detection and prevention of fraud**.

[50] Unfortunately, there are many examples of companies set up shortly before or shortly after the launch of a public tender for funding under EU support programmes, which then 'miraculously' manage to receive that funding. In the case of companies set up shortly before the public tender was launched, all the evidence suggests that their owners are either linked to political circles or to individuals holding political office, and that they have access to inside information that gives them an advantage over other applicants.

The combination of such advanced analytics tools with the database containing information concerning patterns of fraud across the EU could be extremely useful to prevent fraud, detect signs of fraud and subsequently establish the commission of offences.

In the case of EDES and Arachne+, which are not equipped with AI technology, it is recommended to add this capability, as this would greatly facilitate the analysis of the data entered. The effectiveness would be further enhanced if the data entered into EDES and Arachne+ were cross-referenced with the data entered in the database on fraud patterns referred to above. These tools should also integrate **real-time property transaction data to detect risk patterns**, such as acquisitions of high-value properties by recipients of EU funds that are inconsistent with their reported income profiles.

Concerning Arachne+, its use by relevant authorities is currently voluntary. However, it might be useful if its use were made mandatory for managing authorities, as this would improve the chances of detecting fraud.

It is absolutely essential to prevent cyberattacks against databases and programmes designed to prevent, detect and investigate fraud against the EU's financial interests. Cybersecurity is therefore also an essential tool for effectively tackling fraud against the EU's financial interests.

It might also be useful to develop IT tools designed to identify the locations where EU funding is being spent, in order to detect double-funding through applications submitted in different Member States or by different entities (both natural and legal persons). In other words, all subsidised projects must be georeferenced using interoperable coordinates. To increase the level of detection of double-funding, **this data must be cross-referenced with the graphical databases of national Land Registries**. This ensures the physical uniqueness of the property associated with the funding.

e. Further Proposals

With regard to further proposals, firstly, Directive (EU) 2017/1371 includes, as 'Other criminal offences affecting the Union's financial interests' (in addition to fraudulent conduct), corruption (active and passive), money laundering and misappropriation. **However, there are other offences which, for the same reasons as corruption, money laundering and misappropriation, should be considered as 'Other criminal offences affecting the Union's financial interests'**, such as influence peddling, perversion of justice (judicial or administrative), and misconduct in public office (by a member of an authority or public official in the course of a legal transaction, with the intention of obtaining an unlawful advantage for themself or another, regardless of whether or not the public interests that they have a duty to safeguard are negatively affected). Therefore, **a Directive should be adopted so that these offences are added to the list of 'Other criminal offences affecting the Union's financial interests'. The same should apply to offences such as terrorism, financing of terrorism, and participation in or cooperation with a terrorist group or a criminal organisation**[51].

Secondly, given the involvement of criminal organisations and terrorist groups in fraud against the EU's financial interests, the prevention of such fraud is essential for an effective response to organised crime and terrorism. Thus, given the need for a *continuum* between prevention and criminal prosecution, in order to ensure a more effective response to fraud against the EU's financial interests, **it would be**

[51] The commission of a PIF offence within the context of a criminal organisation is provided as an aggravating circumstance in Article 8 of Directive (EU) 2017/1371, and EPPO has competence to investigate and prosecute offences regarding participation in a criminal organisation as defined in Framework Decision 2008/841/JHA, as implemented in national law, if the focus of the criminal activity of such a criminal organisation is to commit any of the offences referred to in Directive (EU) 2017/1371, as well as any other criminal offence that is inextricably linked to criminal conduct that falls within the scope of Directive (EU) 2017/1371. However, the focus of many criminal organisations (perhaps the overwhelming majority) and terrorist groups is not to commit any of the offences referred to in Directive (EU) 2017/1371. Therefore, including offences such as terrorism, financing of terrorism, and participation in or cooperation with a terrorist group or a criminal organisation on the list of PIF offences would help to overcome any obstacles that might arise in practice.

advisable if the same investigative tools that are used in criminal prosecution are also available for use in preventive investigations *ante delictum*. It is also important that the law provides the use of evidence obtained in the context of preventive investigations *ante delictum* in further criminal proceedings, in order to avoid any doubts regarding its admissibility.

For the same reasons, this should also apply to Member States. However, not all Member States have legislation providing the possibility of using, in the context of the prevention of organised crime, terrorism, economic crime and cybercrime, the same investigative measures that are used in criminal proceedings. Thus, **it is recommended to harmonise the Member States' domestic legislation in this regard**. The same applies to the use of evidence obtained in the context of crime prevention in further criminal proceedings.

Finally, in the pre-investigation phase, EPPO should be able to verify information without the data subject being aware thereof. This power must include **expedited access to Land Registry entries and property history**, allowing for a preliminary audit of a suspect's assets without alerting them, thus preventing the concealment of real estate assets.

f. Protection of Fundamental Rights

Naturally, **all these improvements will have to comply with the limitations and safeguards provided in the ECHR (including the case law of the ECtHR), and in EU law, especially the Charter of Fundamental Rights of the European Union, legislation concerning data protection (in particular the GDPR), and the AI Act[52] (including the case law of the CJEU). In fact, EU values and Charter rights must be integrated into all EU legislation.**

For practitioners, it might be recommended to elaborate a Handbook (similar to the one on the European Arrest Warrant) to help facilitate the operation of the legal framework.

[52] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

III. Improving Investigation and Prosecution Capabilities

a. Preliminary Remarks

As mentioned above, detecting and investigating economic crimes is extremely difficult. As fraud against the EU's financial interests is a form of economic crime, **those who commit such crimes – white-collar criminals – are characterised, amongst other things, by their social influence and by being rational criminals who weigh the advantages and disadvantages of committing crimes against law-abiding conduct**[53]. It is often argued that, at least in most cases, white-collar criminals do not lack socialisation, given their socio-economic status, the respectability of their lifestyle and the stability of their place in the community. But this claim must be refuted: economic crime too, even when committed by a white-collar offender, reveals in principle a failure of socialisation, from which arises the State's duty to provide the means for its correction. In fact, white-collar criminals, despite their social status, often have a strong propensity for crime, drawn by the prospect of high and easily obtained profit and confidence that their network of contacts within judicial, political and/or economic circles will shield them from being 'bothered' by the authorities. However, **although in some cases there may be a need to rehabilitate white-collar criminals, the main strategy for combating fraud against the EU's financial interests must be based on deterrence**.

Deterrence tends to be achieved by increasing the risks that criminals face when engaging in fraud, so that the benefits of committing fraud are no longer worth the risk. These risks will be increased if the effectiveness of crime detection, investigation and prosecution is improved and also if offenders can expect the legal consequences of crime (particularly sanctions and confiscation) to be severe[54]. The imposition of severe legal consequences depends on the effectiveness of crime detection, investigation and prosecution.

According to Donald R Cressey, there are three key factors considered to be the drivers of fraud, which are summarised in what is known as the 'fraud triangle':

(a) Opportunity: Even if a person has a motive, they must have the opportunity to commit fraud. The existence of inefficient or inadequate internal control systems can create such an opportunity. Naturally, the presumed likelihood of fraud going undetected is a crucial factor for the perpetrator.

(b) Rationalisation: A person may develop a justification for committing fraud by rationalising their actions, for example, 'it is fair to do this – I deserve this money', 'it is owed to me' or 'I'm just borrowing the money – I'll pay it back later'. The perceived risk of the unlawful act being detected and punished is influenced by will and determination.

(c) Pressure, incentive or financial motive: This is the 'need or greed' factor. Pure greed can often be a strong motive. Pressure, on the other hand, may arise from private financial problems or personal vices.

---

[53] See Duarte Rodrigues Nunes (n 22) p 502-503. See also EPPO, *Annual Report 2023*, https://www.eppo.europa.eu/assets/annual-report-2023/pdfs/EPPO_Annual_Report_2023_en.pdf, p 4.

[54] See Ernest van den Haag, *Punishing Criminals*, *Punishing Criminals Concerning a Very Old and Painful Question*, University Press of America, Lanham and London, 1991, p 115-116, James Q. Wilson, *Thinking about crime*, Edição revista, Vintage Books, New York, 1985, p 118-144, and Duarte Rodrigues Nunes, '*Da admissibilidade da revogação da suspensão da pena de prisão por crime cometido no decurso da suspensão punido com nova pena de prisão suspensa na sua execução: Comentário ao Acórdão da Relação de Lisboa de 20 de fevereiro de 2025 (processo 579/15.2PAMTJ-B.L1-9)*', Revista do Ministério Público, n.º 182, Lisbon, 2025, p 258-259.

In this context, the solution to fraud prevention should stem, on the one hand, from reducing the incentives for fraud, and on the other hand, from the establishment of an internal control system aimed at mitigating the factors that make up the 'fraud triangle'.

As mentioned above, gathering evidence of fraud against the EU's financial interests is extremely difficult, given that the perpetrators are particularly cunning criminals who are very familiar with the environment in which they commit their crimes (which are usually committed in the course of their economic or professional activities), possess very specific knowledge of the financial world or have accomplices who have such knowledge, and often enjoy considerable social influence. Investigation is more complex in cases where criminals use IT resources to commit fraud, as is usually the case. The situation becomes even more complex in cases where fraud is committed by criminal organisations or terrorist groups.

The only way to overcome the enormous challenges of investigating organised crime, economic crime, terrorism, and cybercrime is through the 'infiltration' of criminal or terrorist organisations or unorganised criminal schemes, and/or through cooperation with individuals involved in criminal activity (crown witnesses). 'Infiltration' and cooperation can only be achieved in two ways: either by using covert criminal investigation means[55] (interception of electronic communications, audio and/or visual surveillance, undercover operations, covert computer searches, etc) or by resorting to crown witnesses, thereby breaking the *affectio societatis* (which is based, to a large extent, on the duties of secrecy and non-cooperation with the authorities incumbent upon members and associates of criminal organisations) or the pact of silence existing between the various parties involved (eg, in corruption, the pact of silence between the briber and the bribee)[56].

Therefore, the **effectiveness of the investigation of fraud against the EU's financial interests depends on the authorities being able to use means of obtaining evidence that enable them to 'infiltrate' fraud schemes, and/or secure the cooperation of individuals involved in criminal activity (crown witnesses). The cooperation of whistleblowers and effective cooperation between EPPO and other EU bodies and/or Member States and/or non-EU countries' authorities are also essential**.

A special problem is the access to, and the use of, data collected in other Member States. Digital evidence is not confined to individual States and may be stored on servers in other countries. This necessitates, on the one hand, the ability to access data stored on foreign servers; on the other hand, it raises the question of whether and how evidence obtained abroad can be admitted in criminal proceedings. There are differences in the Member States' rules on the seizure of data, the transfer of data and the admissibility of electronic evidence. On the one hand, differing criminal procedure laws make the acquisition of digital evidence difficult; this causes problems in investigations of transnational fraud cases. On the other hand, however, they also open up opportunities to circumvent national procedural principles, national criminal procedure law or even constitutional law.

Issues relating to the cross-border collection and use of digital evidence cannot be resolved at national level alone. Similarly, for the investigation and prosecution of cases of fraud against the financial interests of the EU, regulations are needed within the EU that provide for common standards for the collection and use of evidence. There is a need to **harmonise the conditions for the collection of digital evidence in the EU**. In doing so, fundamental rights and the need for efficient criminal prosecution will be balanced at the European level. Otherwise, frictions, obstacles to the collection of digital evidence and opportunities for circumvention will be difficult to resolve.

---

[55] Translation of the German expression *verdeckte Ermittlungsmaßnahmen*, which is also used in Portuguese, being translated as *métodos 'ocultos' de investigação criminal*.

[56] See Duarte Rodrigues Nunes (n 4) p 425-426, and 649, and *A Colaboração Premiada*, Gestlegal, Coimbra, 2024, p 30-31.

It will also be important to **harmonise the rules regarding the admissibility of evidence**, given that the Member States' legal systems are significantly different. Differences range from systems that apply very strict exclusionary rules – eg for an infringement of merely formal legal provisions – to systems that apply a balancing test, even in cases where evidence was obtained unlawfully in violation of human rights. These divergences are of crucial importance when evidence is collected abroad. The admissibility of evidence collected abroad will depend on how such evidence has been obtained and which rules have been applied during such a process. While several legal systems require evidence to have been obtained in accordance with the *lex fori* in order to be admissible, other States admit such evidence as long as the *lex loci regit actum* principle has been complied with. There are countries that put their trust blindly in the process through which the evidence was collected abroad and apply the *principle of non-inquiry*: compliance with the formalities or norms governing evidence gathering abroad are not checked and there might not even be a control of the lawfulness of such evidence. There are also countries that automatically exclude evidence that has been obtained in an illegal manner in the country of collection. The diversity of solutions that exist in each of the Member States hinders the establishment of what has been called 'an area of free movement of criminal evidence' and, on the other hand, may also have a negative impact on the rights of the defence[57]. **In this regard**, **ELI has submitted a Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings**[58].

b. Improving Complementarity between EPPO and OLAF Investigations

The terms of the working arrangement between EPPO and OLAF[59] appear to be appropriate. However, it is absolutely essential that OLAF always acts as an independent body, and never as an extension of the Commission[60]. As mentioned in the White Paper for the Anti-fraud Architecture Review, the use of complementary administrative investigations has remained rather limited so far, although both types of investigations (criminal and administrative) are essential and contribute to fully protecting the EU budget and prevent or limit damage.

One main problem seems to be that the working methods of OLAF and EPPO do not complement each other sufficiently. The reason for this appears to be, on the one hand, that OLAF's reports are forwarded to EPPO too late and, on the other hand, that the reports and material sent do not meet the requirements necessary for criminal prosecution. These problems are not entirely new. Similar experiences were also reported by national public prosecution authorities.

Criminal investigations must be carried out and finalised as fast as possible, ideally shortly after the offence has been committed or after it has come to light. Therefore, criminal prosecution authorities need incriminating evidence quickly. If OLAF's reports are submitted too late, this delays criminal proceedings and may also lead to the offences becoming time-barred. In general, long criminal proceedings make

---

[57] See European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings*, Vienna, 2023, https://www.europeanlawinstitute.eu/projects-instruments/instruments/, p 12.

[58] *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings*, cited above.

[59] Working Arrangement between the European Anti-Fraud Office and the European Public Prosecutor's Office, 5 July 2021, https://www.eppo.europa.eu/sites/default/files/2021-07/Working_arrangement_EPPO_OLAF.pdf.

[60] In this particular case the sentence: 'EU law provides for a sincere and effective cooperation between the Commission through OLAF and the Member States' competent authorities, as well as for OLAF supporting EPPO's criminal cases or complementing them with administrative investigations', on page 6 of the White Paper, gives cause for concern, insofar as OLAF seems to be understood as an extension of the Commission. If understood in this way, it becomes very difficult to involve OLAF in investigations, as this can only happen if OLAF is and acts as a body that is truly independent of the Commission.

investigations and the gathering of evidence more difficult. Therefore, **provisions should be foreseen that OLAF has to transmit all available relevant information to EPPO without delay**.

Without prejudice to what has already been mentioned regarding the improvement of cooperation between EPPO and OLAF, it is recommended to **amend the EPPO Regulation to provide the possibility for EPPO to carry out preventive investigations *ante delictum***. **Given that EPPO focuses on criminal liability**, **and OLAF focuses specifically on gathering the data necessary for the early recovery of defrauded funds**, **the possibility of EPPO to carry out preventive investigations *ante delictum* could increase the number of situations in which EPPO investigations could be complemented by administrative investigations conducted by OLAF**.

In fact, Commission's White Paper distinguishes between prevention and detection phases of conduct that harms the EU's financial interests and the investigation phase. Detection and prevention undoubtedly fall to frontline agents, such as fund management authorities (regarding expenditure) or tax authorities (regarding revenue). However, it is important to recognise the existence of a pre-investigation phase, which corresponds to the verification phase prior to the initiation of a criminal investigation. Therefore, EPPO should be able to collect information, secretly and expeditiously, regarding potential offences that come to its attention, either through judicial cooperation mechanisms (when a delegation fulfils a cooperation request issued by another, it may become aware of a potential PIF offence in its territory and must be able to verify it) or through fortuitous means (newspaper articles, television reports, anonymous complaints). In this phase, if there is no possibility to consult banking or tax information, the powers in question will be null and void. A safeguard clause may be applicable that stipulates the destruction of the obtained documents if a criminal investigation is not initiated.

Investigations aimed at tracing and identifying proceeds of crime and other crime-related property relating to fraud against the EU's financial interests, and other criminal offences affecting the Union's financial interests which may become the object of a freezing, seizing or confiscation order are carried out by the Member States' asset recovery offices. Given OLAF's acquired expertise on gathering the data necessary for the early recovery of defrauded funds, **it could be useful to grant it the power to conduct**, **under the supervision of EPPO**, **complementary investigations aimed at mitigating damage to the EU's financial interests and tracing and identifying proceeds of crime and other crime related property relating to fraud against the EU's financial interests**, **and other criminal offences affecting the Union's financial interests which may become the object of a freezing**, **seizure or confiscation order**. It is important to assess the relationship between the PIF Directive and other EU law instruments that deal specifically with asset recovery. For example, Directive (EU) 2024/1260 lays down minimum rules on the tracing, identification, freezing, confiscation, and management of property in criminal proceedings. This Directive mainly focuses on the Member States but also concerns cooperation with EPPO and third countries. Therefore, this issue on EPPO's role vis-à-vis OLAF with regard to asset recovery, as well as the impact of the Directives that deal with asset recovery, should be clarified further.

However, **administrative investigations may entail serious procedural risks of the *nemo tenetur* principle violation**, **which are similar to those arising from conducting tax audits** (**in which there are duties of active cooperation on the part of those concerned**) **simultaneously with criminal investigations**. Therefore, it is essential to have safeguards aimed at preserving the *nemo tenetur* principle, even if it is not an absolute principle. **One possibility for safeguarding the *nemo tenetur* principle would be to equate OLAF's actions with the actions of a Criminal Police Agency**.

c. Improving Access to and Exchange of Fraud-Related Data

As mentioned above, due to social, economic, cultural or legislative factors, as well as the way in which the authorities operate, among others, each country has its own peculiarities in terms of fraud, it is therefore extremely important that both the competent authorities of the Member States and AFA actors are aware of the *modi operandi* of fraudsters operating

within Member States or even in non-EU countries, engaging in conduct likely to harm the EU's financial interests. In addition, in each Member State, fraud against the EU's financial interests may be committed either by individuals from that Member State or by individuals from another Member State or from non-EU countries.

Therefore, **a database that is directly**[61] **accessible both to AFA actors and to the Member States' authorities responsible for preventing and combating fraud against the EU's financial interests, and other criminal offences affecting the Union's financial interests containing information concerning *modi operandi* of fraudsters operating within Member States or even in non-EU countries, engaging in conduct likely to harm the EU's financial interests, would enhance not only fraud prevention and early detection, but also criminal investigations into fraud against the EU's financial interests, and other criminal offences affecting the Union's financial interests. Direct access to this database, rather than having to request access (even through fast-track procedures), will enable information contained in the database to be accessed more effectively and quickly, which will result in greater efficiency in fraud investigations and in the adoption of administrative measures or measures of another nature, in particular, measures relating to criminal proceedings.**

However, as also mentioned above, insofar as the data contained in that database may include personal data, **the requirements laid down in data protection legislation, in particular the GDPR, must be met.**

It could also be useful to establish, through legislation, mechanisms for access to information (as suggested above, in the case of EPPO, regarding the broadening of the scope of Article 43 of the EPPO Regulation) alongside mandatory reporting mechanisms. The information could be centralised in one entity, namely EPPO or Europol.

d. Leveraging New Technologies and AI

As mentioned above, the **detection of signs of fraud often requires the analysis of a very large volume of data. This data may consist of information already held by the authorities or data that is freely available on the internet.** Therefore, the **use by both EU and Member States' authorities of advanced analytics tools using AI, machine learning, and complex modelling to uncover hidden information and provide predictive insights that are capable of detecting and analysing digital data that may be relevant to the detection of signs of fraud and to the subsequent establishment of the commission of offences tends to be essential both for the detection and prevention of fraud.**

The combination of such advanced analytics tools with the database containing information concerning patterns of fraud across the EU could be extremely useful to prevent fraud, detect signs of fraud and subsequently establish the commission of offences.

In the case of EDES and Arachne+, which are not equipped with AI technology, it is recommended to add this capability, which would greatly facilitate the analysis of the data entered. The effectiveness would be further enhanced if the data entered into EDES and Arachne+ were cross-referenced with the data entered in the database on fraud patterns referred to above.

---

[61] With regard to direct access to this database by bodies (eg OLAF) whose actions may be equated with the actions of those of a Criminal Police Agency, such data was collected/obtained for the purposes of crime prevention and/or prosecution of criminal offences. In such situations, for example, OLAF is acting within the scope of its powers to prevent and detect fraud against the EU's financial interests, and there is no deviation from the purpose for which the data was obtained/collected. Indeed, a very similar situation can be found in the case of automated data matching with available data (*Datenabgleich*) provided in Section 98c of the German Code of Criminal Procedure. According to Section 98c of the German Code of Criminal Procedure, 'In order to investigate an offence or to determine the whereabouts of a person sought in connection with criminal proceedings, personal data from criminal proceedings may be automatically matched with other data stored for the purposes of criminal prosecution or enforcement of sentence, or in order to avert a danger. (…)'. Because of this, automated data matching with available data may be used to investigate any crime and is carried out by the Public Prosecutor's Office or by the police under the 'general investigation clause' (*Ermittlungsgeneralklausel*) provided in §§161 and 163.

Concerning Arachne+, its use by managing authorities is currently voluntary. However, it might be useful if its use were made mandatory for managing authorities, as this would improve the chances of detecting fraud. **It is absolutely essential to prevent cyberattacks against databases and programmes designed to prevent, detect and investigate fraud against the EU's financial interests. Cybersecurity is therefore also an essential tool for effectively tackling fraud against the EU's financial interests.**

It might also be useful to develop IT tools designed to identify the locations where EU funding is being spent, in order to detect double-funding through applications submitted in different Member States or by different entities (both natural and legal persons).

In fact, in criminal proceedings, AI could be used to search through the vast amount of data collected during criminal proceedings and filter out the information relevant for the criminal prosecution in a certain case, which could save time. At the same time, care must be taken to ensure that final decisions are taken by a human on whether or not to prosecute or convict individuals. Therefore, on the one hand, a legal framework must be established on how to use AI in criminal proceedings and to define its limits. On the other hand, adequate Knowledge Infrastructure (KI) tools should be developed and made available to AFA actors, particularly to prosecution authorities.

e. Effectiveness of Investigation and Prosecution of PIF Crimes

With regard to improving the effectiveness of the investigation of PIF offences, given the increasing use of computer technology in the commission of fraud against the EU's financial interests, it is essential to improve and harmonise[62] Member States' domestic legislation on the gathering of digital evidence. Improving the legislation will provide the authorities with more effective investigative tools, which could lead to more effective investigations. The harmonisation of Member States' legislation will eliminate gaps and inconsistencies between Member States' domestic laws, which, where they exist, seriously undermine international cooperation in criminal matters and, consequently, the effectiveness of investigations and the administration of criminal justice.

In fact, with regard to the European Investigation Order (EIO), Article 6(1)(b) of Directive 2014/41/EU[63] provides that the issuing authority may only issue an EIO in cases where the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case.

Firstly, in EncroChat and Sky ECC cases, despite all the secrecy that has surrounded and continues to surround the way in which the French authorities obtained communications content data via EncroChat and SKY ECC, everything indicates that such data was obtained through the bulk interception of communications[64], more specifically through bulk source surveillance[65] (as the French authorities used malware to gain access to the phones of EncroChat and SKY ECC customers). Given the high level of encryption used in communications carried out via communications network and service providers similar or even more sophisticated than EncroChat and Sky ECC (which were shut down by the authorities), these communications services are particularly attractive to criminals. However, they may also be used by others (eg, investigative journalists, political activists or company employees who are concerned

---

[62] As mentioned in European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings*, cited above, p 12, the rules concerning evidence in criminal proceedings differ significantly at national level, including at the stage of evidence gathering, where some countries require a minimum gravity of the crime to adopt certain investigative measures or a prior judicial warrant, while others are more flexible in allowing measures that encroach on fundamental rights. The differences stem largely from diverging structures of criminal proceedings and, in particular, the powers of law enforcement and prosecution bodies at the pre-trial stage and the significance of the adversarial principle.

[63] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[64] See Judgments of the CJUE (Grand Chamber) of 30 April 2024 and of the Berlin Regional Court of 19 December 2024.

[65] Translation of the German expression *Quellenüberwachung*.

about industrial espionage) for legitimate purposes[66]. Nevertheless, **bulk interception is becoming an increasingly necessary tool for both criminal investigation and crime prevention**. Therefore, particularly given the growing involvement of criminal organisations and terrorist groups in such fraud, bulk interception is becoming an increasingly necessary tool also for both prevention and investigation of fraud against the EU's financial interests. Given that, due to its scope, bulk interception restricts fundamental rights more intensely than targeted interception, the ECtHR has handed down several judgments on the matter, in particular regarding the conditions under which it may be carried out[67] and the guarantees and safeguards relating to due process[68] under the ECHR. The CJEU ruled that the EncroChat data can be admissible evidence in the EU, provided that certain conditions are met[69].

Bulk interception should therefore be provided in the domestic legislation of all Member States, whilst complying with the conditions laid down by the case law of the ECtHR and the CJEU in this regard. In addition, any restrictions arising from the constitutions of the Member States must also be taken into account.

Secondly, Voice over Internet Protocol (VoIP) enables voice and multimedia communications over the internet rather than traditional telephone lines. It converts analogue voice signals into digital data packets, transmitting them via broadband, allowing calls via desktop computers, VoIP phones, or mobile apps. It is therefore necessary to intercept communications before they are encrypted or after they have been decrypted, which requires the use of malware to gain access to the computer systems used for communication (source surveillance). **Given the widespread use of VoIP communications, source surveillance is a necessary investigative tool for both prevention and investigation of fraud against the EU's financial interests.** However, there are Member States whose domestic legislation does not expressly provide either source surveillance or the use of malware to intercept communications. Therefore, **both the use of source surveillance and the use of malware to intercept communications should be provided in the domestic legislation of all Member States. Naturally, the legal framework for source surveillance will have to comply with the limitations and safeguards provided in the ECHR (including the case law of the ECtHR), and in EU law, especially the Charter of Fundamental Rights of the European Union and legislation concerning data protection (including the case law of the CJEU). In addition, any restrictions arising from the constitutions of the Member States must also be taken into account.**

Thirdly, the success of many criminal investigations (particularly in the case of investigations into organised crime, terrorism, economic crime and cybercrime) depends on the suspects remaining unaware that they are under investigation. And, as IT tools are increasingly used to commit crimes, the covert gathering of digital evidence is becoming ever more essential to the success of many investigations. Thus, **covert computer searches or online searches[70] are becoming ever more essential to the success of many investigations**. Covert computer searches consist of covert access to a computer system for the purpose of observing or monitoring its use and searching, and possibly copying, the data stored on it or accessible via it. Covert computer searches may involve a single instance of access (data mirroring) or take place on a continuous and prolonged basis (data monitoring)[71]. However, there are Member States whose domestic legislation does not expressly provide either covert computer searches or the use of malware in computer searches. **Given the**

---

[66] See Judgment of the Berlin Regional Court of 19 December 2024.

[67] See Judgements of the ECtHR (Grand Chamber) *Big Brother Watch and Others v. the United Kingdom*, and *Centrum för rättvisa v. Sweden*, both of 25 May 2021.

[68] See Judgments of the *ECtHR Yüksel Yalçinkaya v. Türkiye* (Grand Chamber), of 26 September 2023, and *Sigurđur Einarsson and Others v. Iceland*, of 4 June 2019.

[69] See Judgement of the CJUE (Grand Chamber) of 30 April 2024.

[70] Translation of the German expression *Online-Durchsuchung*.

[71] See Duarte Rodrigues Nunes, '*Da admissibilidade da utilização de benware no Direito português*', Ciberlaw, n.º 10, Lisbon, 2020, https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_10.pdf, p LXXVIII.

widespread use of computer technology to plan, commit, and/or erase traces of crimes, or to store information that may be relevant to criminal investigations, covert computer searches are a necessary investigative tool for both the prevention and investigation of fraud against the EU's financial interests. Naturally, **also the legal framework for covert computer searches will have to comply with the limitations and safeguards provided in the ECHR (including the case law of the ECtHR), and in EU law, especially the Charter of Fundamental Rights of the EU and legislation concerning data protection (including the case law of the CJEU). In addition, any restrictions arising from the constitutions of the Member States must also be taken into account**.

Fourthly, given that the need to analyse large amounts of data is becoming increasingly common in criminal investigations and the use of AI is a tool that greatly facilitates the analysis of large amounts of data (without prejudice to subsequent analysis carried out by experts), **the possibility and the conditions for using AI in the context of criminal investigations should be clarified in the domestic law of Member States**.

As mentioned above, in criminal proceedings, AI can be used to search through the vast amount of data collected during criminal proceedings and filter out the information relevant for the criminal prosecution in a certain case, which could save time. At the same time, care must be taken to ensure that AI does not make final decisions on whether or not to prosecute or convict individuals. Therefore, on the one hand, a legal framework must be established on how to use AI in criminal proceedings and to define the limits of its use. On the other hand, adequate KI tools should be developed and should be made available to AFA actors, particularly to prosecution authorities.

Fifthly, there is an increasing need to rely on crown witnesses to prove the commission of crimes in the context of organised crime, terrorism and even economic crime. However, there are significant discrepancies between the domestic legislation of the Member States regarding crown witnesses. Therefore, **given that the use of leniency programmes involving individuals participating in criminal activities is essential in the investigation of fraud against the EU's financial interests, it is recommended to harmonise the domestic legislation of the Member States so such individuals have an adequate and comprehensive legal framework for crown witnesses, both in terms of effectiveness in preventing and combating crime and effectiveness in procedural safeguards for suspects and crown witnesses**.

Sixthly, following the Digital Rights judgment[72] and the case law (both of the CJEU and of the courts of the Member States) that followed it, the retention of metadata for the purposes of criminal investigations and its use as evidence has encountered enormous obstacles, which have resulted in many criminal investigations proving ineffective[73]. Metadata relating to traffic, location and subscriber data tend to be highly relevant in investigations into fraud affecting the EU's financial interests. The aforementioned obstacles relating to metadata retention for the purposes of criminal investigations and its use as evidence may therefore also jeopardise the success of investigations into fraud affecting the EU's financial interests. Thus, **the reintroduction of an EU-wide framework for metadata retention obligations for the purposes of criminal investigations would be particularly useful in order to improve the effectiveness of the investigation of fraud affecting the EU's financial interests**.

---

[72] See Judgment of the CJUE (Grand Chamber) Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others of 8 April 2014, C293/12 and C594/12.

[73] Criticising the CJEU and the Portuguese Constitutional Court's case law regarding metadata retention for the purposes of criminal prevention and investigation, Duarte Rodrigues Nunes, '*Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor*?', Revista do Ministério Público n.º 170, Lisbon, 2022, p 9-58, and 'O *Day After* do Acórdão do Tribunal Constitucional n.º 268/2022', *Privacidade e Proteção de Dados do Município de Lisboa*, Câmara Municipal de Lisboa, Lisbon, 2024, p 171-244.

Seventhly, with regard to forensic investigations, EPPO generally relies on the forensic police units of each Member State and, in exceptional cases, on OLAF. However, in order to expedite the progress of investigations, particularly in cross-border investigations, **it is recommended for EPPO to have an EU body at its disposal to carry out forensic analyses in the context of investigations into fraud affecting the Union's financial interests and other criminal offences affecting the Union's financial interests**. That body could be Europol, which should be provided with the necessary resources.

Eighthly, although AFA actors can already access each other's databases, the conditions under which such access and data-sharing take place can be improved still further. Thus, as proposed in the White Paper for the Anti-fraud Architecture Review, it is recommended to allow OLAF and EPPO to exchange information with EU VAT Fraud Prevention Network (Eurofisc) and provide them with centralised access at EU level to certain VAT information so that they can investigate potential fraud or VAT-related irregularities[74]. In other words, **it is recommended to broaden the scope of Article 43 of the EPPO Regulation in order to allow EPPO expedited access to information held by EU and Member States' institutions**.

Ninthly, the domestic law of several Member States provides the possibility of waiving bank and tax secrecy by decision of the public prosecutor. Insofar as this does not involve severe restrictions on fundamental rights, **it would be useful to harmonise legislation in this regard**, **which would enable EPPO to order the waiver of bank secrecy and tax secrecy in investigations into fraud affecting the Union's financial interests and other criminal offences affecting the Union's financial interests**.

Tenthly, if not all Member States have a central register of bank accounts, **it is recommended to harmonise Member States' national legislation with a view to establishing a central register of bank accounts**, which would facilitate the cross-referencing of information relevant to the prevention, detection and investigation of fraud against the EU's financial interests.

Eleventhly, the domestic legislation of some Member States does not provide GPS geolocation for the purposes of criminal investigations, which raises doubts as to its admissibility. GPS geolocation can be extremely useful in investigating VAT-related fraud, for example, in detecting falsified documentation on the international transportation of goods (where, in reality, the transport in question took place between two points within the territory of the same Member State). GPS geolocation can also be extremely useful in detecting double-funding situations. As mentioned above, all subsidised projects must be georeferenced using interoperable coordinates. To increase the level of detection of double-funding, **this data must be cross-referenced with the graphical databases of national Land Registries**. This ensures the physical uniqueness of the property associated with the funding. Therefore, **it is recommneded to harmonise the domestic legislation of the Member States so that the use of GPS geolocation is provided in the domestic legislation of all Member States**.

Finally, as mentioned above, in the pre-investigation phase, EPPO should be able to verify information without the data subject being aware thereof. This power must include **expedited access to Land Registry entries and property history**, allowing for a preliminary audit of a suspect's assets without alerting them, thus preventing the concealment of real estate assets.

With regard to improving the effectiveness of the prosecution of PIF offences, the White Paper for the Anti-fraud Architecture Review proposes:

(a) At national level, dedicated and specialised law enforcement authorities could support EPPO more effectively, in particular in areas such as customs, tax fraud, and financial crime; and

(b) At EU level, an increased cooperation between EPPO and Europol as regards risk analysis and

[74] See European Commission, *White Paper for the Anti-fraud Architecture Review*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0546&qid=1753799750304, pp 6-7.

operational support, and between EPPO and Eurojust as regards the functioning of the Joint Investigation Teams (JITs), which would allow greater support to EPPO, particularly in cross-border cases. In addition, a semi-automated hit/no-hit system tailored for EPPO, Eurojust, Europol, and OLAF, which, while respecting procedural guarantees and mandates of each of the bodies and agencies, could improve the early detection of cross-border criminal patterns and facilitate cooperation.

These proposals appear to be highly appropriate for improving the efficiency of the prosecution of PIF offences. However, another proposal could be formulated. Given that, as mentioned above, specialised law enforcement authorities should support EPPO, this cooperation could formally include **Registry-based Anti-Money Laundering Centres**, which could provide expert analysis on suspicious real estate movements and complex corporate-property structures.

f. Ensuring the Protection of Fundamental Rights

Naturally, **all these improvements will have to comply with the limitations and safeguards provided in the ECHR** (**including the case law of the ECtHR**), **and in EU law**, **especially the Charter of Fundamental Rights of the European Union**, **legislation concerning data protection** (**in particular the GDPR**), **and the AI Act** (**including the case law of the CJEU**). **In fact**, **EU values and Charter rights must be integrated into all EU legislation**.

As mentioned above, **for practitioners**, **it might be helpful to have a Handbook** (**similar to the one on the European Arrest Warrant**) **to help facilitate the operation of the legal framework**.

IV. Making the Recovery Process More Efficient

a. Preliminary Remarks

Regarding fraud against the EU's financial interests, **asset recovery serves several purposes**. **Firstly**, **it enables the EU to recover revenue of which it has been unlawfully deprived** (**eg in cases of VAT-related fraud**) **and which is necessary for the pursuit of the EU's objectives. Secondly, it enables the EU to recover funding that was wrongly granted to fraudsters**, **allowing it to be used for the purposes not intended under that funding programme**. **Thirdly**, **if criminals are able to retain the proceeds of crime, the deterrent effect of criminal sanctions tends to be diminished**; **therefore**, **asset recovery reinforces the deterrent effect of the sanctions imposed on criminals**. **Fourthly**, **asset recovery prevents offenders from benefiting from the proceeds of crime**, **restores the legal order of assets and prevents assets obtained through criminal activity from being reinvested in further criminal activities**[75].

The objectives of asset recovery are not achieved merely by issuing a confiscation order. **It is necessary to ensure the effectiveness of such orders by tracing**, **seizing and freezing assets**[76]. This requires, first and foremost, appropriate legislation. With the transposition of Decision 2007/845/JHA[77] and Directive 2014/42/EU[78], and the forthcoming transposition of Directive (EU) 2024/1260[79], the domestic law of Member States will provide appropriate mechanisms to trace, seize and freeze assets and order the confiscation of such assets. However, **Directive** (**EU**) **2024/1260 merely lays down minimum rules**: **consequently**, **the adoption of minimum rules does not prevent Member States from granting more extensive powers to asset recovery offices**, **from providing for more extensive rules on freezing and confiscation** (**such as the confiscation of unjustified wealth with a reversal of the burden of proof or civil confiscation**[80]), **or from providing for additional safeguards under national law**, **provided that such national measures and provisions do not undermine the objectives of the Directive**.

b. Protecting the EU Budget through Precautionary and Recovery Measures

The answer to this question depends on an understanding of how Authorising Officers by

---

[75] Regarding the importance of the effectiveness of confiscating the proceeds of crime for more effective crime prevention and repression, see Duarte Rodrigues Nunes (n 22) p 793-794, and '*El decomiso de ganancias como instrumento para la lucha contra la criminalidad organizada, terrorismo, criminalidad económica y ciberdelincuencia*', Consinter – Revista Internacional de Direito n.º XVI, Editorial Juruá, Curitiba e Porto, 2023, https://revistaconsinter.com/index.php/ojs/1611.

[76] For real estate, **immediate electronic communication with Land Registries must be established to execute preventive annotations** (**caveats**) of seizure or prohibitions to dispose, preventing the transfer of assets to protected third parties.

[77] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime.

[78] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

[79] Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation.

[80] The ECtHR has held that the confiscation of unjustified wealth with a reversal of the burden of proof and civil confiscation are admissible under Article 6 of the ECHR and Article 1 of Protocol No. 1 to the ECHR, provided that it complies with the requirements set by the Court (see *Phillips v. The United Kingdom*, of 5 July 2001, regarding confiscation of unjustified wealth with a reversal of the burden of proof, and *Gogitidze and Others v. Georgia*, of 12 May 2015, regarding civil confiscation).

Delegation (AODs) work, which is only available to those who currently hold, or have previously held, such roles.

c. Facilitating Recovery of Assets and Proceeds

Given that many insolvency cases are fraudulent, with the aim of allowing the alleged insolvent parties a fresh start free of debts, **it is important to rethink the view that is typically embedded in insolvency legislation**: **the view that**, **when filing for voluntary insolvency**, **the alleged insolvent is admitting facts that are unfavourable to them**. **It might therefore be worth considering the possibility of placing the burden of proof regarding the insolvency situation on the alleged insolvent also in these cases**.

Furthermore, **there are many cases of culpable insolvency that are not detected** by the courts and the number of insolvencies classified as culpable is negligible. It is true that the court's investigative powers in insolvency proceedings are those of civil proceedings and that creditors or the insolvency practitioner do not always bring to the court's attention facts that would lead to the conclusion that the insolvency can be classified as culpable.

Therefore, in cases involving insolvency proceedings where claims relate to fraud against the EU's financial interests, **it is recommended for the AFA bodies** (**namely EPPO and OLAF**), **upon becoming aware of the existence of the insolvency proceedings – which they may be informed of by the authorities of the Member States**, **with reporting obligations to be established – to provide the insolvency proceedings with information and/or evidence they have obtained or gathered which suggests that the insolvency should be classified as culpable**.

Classifying the insolvency as culpable may be useful in facilitating the recovery of assets, since such a classification typically leads to the liability of persons other than the insolvent party (*de jure* or *de facto* directors, certified accountants, statutory auditors, persons with a special relationship to the insolvent party or its owners or directors, or other persons who have contributed to the insolvency or its worsening) for the debts arising from the insolvency, with their assets becoming liable for such debts. Similarly, classifying an insolvency as culpable also tends to result in the extinction of the claims that such persons held against the insolvent party.

Given that, **in many insolvency cases**, **the insolvency is caused or aggravated with the complicity of persons other than the insolvent entity or its owners or directors**, **it is recommended to provide for a sufficiently broad list of persons who should be held financially liable for the payment of the insolvency debts**, **provided they have acted with intent or gross negligence**. **It might therefore be useful to promote the harmonisation of Member States' domestic legislation in this regard**.

Another way of improving the recovery of assets could be to **set up an EU agency tasked with selling assets linked to fraud against the EU's financial interests that have been seized or confiscated**[81]. Selling these assets at EU level, rather than at the level of the Member State where the proceedings took place, could lead to more favourable prices being obtained.

Concerning leveraging EPPO's role in criminal proceedings to support the recovery of such assets in favour of the Union's budget, there is also an important discussion about EPPO's role in asset recovery. **It is important to assess the relationship between the PIF Directive and other EU law instruments that deal specifically with asset recovery**. **For example**, **Directive** (**EU**) **2024/1260 lays down minimum rules on the tracing**, **identification**, **freezing**, **confiscation**, **and management of property in**

[81] We are referring to cases where it is not possible to confiscate the assets constituting the proceeds of crime in kind (where the confiscation of those assets is replaced by the confiscation of other assets that can cover the debt arising from the confiscation order). In the case of assets which themselves constitute the proceeds of crime, such assets do not form part of the debtor's property for the purposes of the insolvency proceedings.

criminal proceedings. **This Directive mainly focuses on the Member States but also concerns cooperation with EPPO and other third countries**. **Therefore**, **the question of EPPO's role vis-à-vis OLAF with regard to asset recovery**, **as well as the impact of the Directives that deal with asset recovery**, **should be clarified further**.

d. Strengthening Deterrence

Given that fraud against the EU's financial interests is a form of economic crime, those who commit such crimes – white-collar criminals – are characterised, amongst other things, by their social influence and by being rational criminals who weigh the advantages and disadvantages of committing crimes against law-abiding conduct[82].

Although in some cases there may be a need to rehabilitate white-collar criminals, the main strategy for combating fraud against the EU's financial interests must be based on deterrence. Deterrence will tend to be achieved by increasing the risks that criminals face when engaging in fraud, so that the benefits of committing fraud are no longer worth the risk. These risks will be increased if the effectiveness of crime detection, investigation and prosecution is improved and also if offenders can expect the legal consequences of the crime (particularly sanctions and confiscation) to be severe[83]. The imposition of severe legal consequences depends on the effectiveness of crime detection, investigation and prosecution.

Regarding asset recovery, if the perpetrator, even after being punished by a criminal sanction, was able to enjoy the profits obtained through the commission of crimes (which they could never, or only with great difficulty, have obtained by lawful means), they would have achieved the objectives they sought by committing the crimes. In such situations, any criminal sanctions that might be imposed would tend to be regarded by criminals as a lesser evil, which would seriously undermine the effectiveness of criminal sanctions. **It is therefore essential that the application of criminal sanctions be accompanied by the confiscation of the proceeds of crime**. **However**, **confiscation cannot be limited to the mere issuance of a confiscation order**. **It is also imperative that the confiscation order be effectively enforced and that criminals be effectively deprived of the assets they have obtained through the commission of crimes**, **which can only be achieved through the effective tracing**, **seizure and freezing of assets that constitute the proceeds of crime**.

In any case, it must be emphasised that the **effectiveness of asset recovery depends primarily on the effectiveness of the detection and prevention of crimes**. However, in many cases, it also depends on the criminal investigation and prosecution. In such situations, **it is absolutely essential that the evidence obtained during the criminal investigation is also used for the purposes of the confiscation order**.

Furthermore, it should be borne in mind that the difficulties inherent in (criminal) investigations into organised crime, terrorism, economic crime and cybercrime also apply to the tracing, seizure and freezing of assets that constitute the proceeds of crime.

Investigations aimed at tracing, seizing and freezing assets for the purposes of confiscation in cases of fraud against the EU's financial interests are carried out by the asset recovery offices of the Member States. However, the asset recovery offices of the Member States are required to carry out such investigations both in cases falling within the competence of EPPO and in cases falling within the competence of the public prosecutors' offices of the Member States, which may compromise the effectiveness of the tracing, seizure and freezing of assets that are, or have been, the subject of a confiscation order. It could therefore be useful to provide the possibility,

---

[82] See Duarte Rodrigues Nunes (n 22) p 502-503. See also EPPO, *Annual Report 2023*, https://www.eppo.europa.eu/assets/annual-report-2023/pdfs/EPPO_Annual_Report_2023_en.pdf, p 4.

[83] See Ernest van den Haag (n 54) p 115-116, James Q. Wilson, (n 54) p 118-144, and Duarte Rodrigues Nunes (n 54) p 258-259.

within the framework of the AFA, of conducting investigations, in parallel with EPPO investigations or in the context of the enforcement of a confiscation order, aimed at tracing, seizing and freezing assets for the purposes of confiscation.

It has been discussed whether authorities may use investigative means that are provided by law solely for the purposes of criminal investigations also in investigations aimed at tracing, seizing and freezing the proceeds of crimes. However, as mentioned above, the **specific difficultes inherent in the criminal investigation of organised crime**, **terrorism**, **economic crime and cybercrime are also encountered in investigations aimed at tracing**, **seizing and freezing proceeds of crimes committed within the scope of these forms of criminality**. **Thus**, **in many cases of fraud against the EU's financial interests**, **tracing**, **seizing and freezing proceeds of crimes is only possible if the authorities use investigative means that are provided by law solely for the purposes of criminal investigations**. **Therefore**, **given the inextricable link between the confiscation of proceeds of crimes and the application of criminal sanctions for the purpose of responding to organised crime**, **terrorism**, **economic crime and cybercrime**, **it is recommended to harmonise the Member States' domestic legislation by providing the possibility of using investigative methods that are usually only admissible for the purposes of criminal investigations also in the context of investigations aimed at tracing**, **seizing and freezing the proceeds of crimes**. **Consequently**, **all the proposals set out above**, **the aim of which is to improve the effectiveness of the detection**, **prevention**, **investigation and prosecution of the EU's financial interests**, **should also be implemented for the purposes of asset recovery**.

V. Improving the Governance of the Anti-Fraud Architecture

The answer to questions concerning improving the governance of the anti-fraud architecture depends on an understanding of how AODs work, which is only available to those who currently hold, or have previously held, such roles. Nevertheless, it is important that the complex web of legislative measures that regulate similar areas also align with the principles of better regulation and that the EU applies the subsidiarity test and effectiveness, and hence ensures transparency and legitimacy.

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9505990-3-9