Pázmány Law Working Papers
2025/12

# Kata Németh
# The current developments in European criminal cooperation - present and future potential competences of the European Public Prosecutor's Office

Pázmány Péter Katolikus Egyetem
Pázmány Péter Catholic University Budapest
http://jak.ppke.hu
http://www.plwp.eu/
ISSN: 2062-9648

**The current developments in European criminal cooperation - present and future potential competences of the European Public Prosecutor's Office**

KATA NÉMETH[1]

## Abstract

This paper examines the establishment and evolving role of the European Public Prosecutor's Office (EPPO) in safeguarding the financial interests of the European Union. It highlights the crucial challenges the EPPO faces, particularly regarding cybercrime and the cross-border nature of modern offenses involving EU funds and financial interest. In evaluating the added value of the EPPO, the analysis assesses its jurisdictional deficiencies and potential for expansion of competences into areas such as cyber-enabled fraud and related organized crime. The paper underlines the necessity for increased harmonization of substantive criminal laws among Member States to advocate the EPPO's effectiveness. Finally, it proposes possible reforms to strengthen investigative capacities and asset recovery, positioning the EPPO as a frontline actor in European criminal cooperation.

## 1. Introductory thoughts

The establishment of the European Public Prosecutor's Office has been a milestone in the criminal justice integration of the European Union, in particular in the protection of the EU's financial interests. In today's dynamically changing crime landscape, cybercrime is a particularly rapidly evolving and increasingly complex challenge. Crimes committed using digital tools, such as misuse of EU funds, phishing or online money laundering, increasingly affect the financial interests of the European Union, while the effectiveness of action by Member States is limited. This raises the question of the future extension of the EPPO's competence to cybercrime and the necessity to the EPPO to place increasing emphasis on the tracing, freezing and recovery of criminal assets.

The aim of this study is to provide an overview of the challenging functioning of the European Public Prosecutor's Office, which is responsible for protecting the financial interests of the Union, and to highlight the shortcomings in its jurisdiction and evaluate the possibilities for extending its powers to fight cybercrime. The paper examines the potential for the EPPO to be a victim of cybercrime and the role of the EPPO in the system of combating cybercrime and

[1] Assistant judge, Criminal Division of the Budapest Capital Regional Court, European Legal Adviser; PhD student at the Doctoral School of Law and Political Sciences of Pázmány Péter Catholic University; SUPPORTED BY THE EKÖP-24-3 UNIVERSITY RESEARCH SCHOLARSHIP PROGRAM OF THE MINISTRY FOR CULTURE AND INNOVATION FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND

European criminal cooperation. The paper identifies problems, proposes solutions to these problems and concludes with a comprehensive set of conclusions.

## 2. Establishment of the European Public Prosecutor's Office

The establishment of the European Public Prosecutor's Office (hereinafter: EPPO) dates back a long way in time to Corpus Juris[2] , and was prompted by the growing need for effective and unified action against crimes against the financial interests of the Union and the realisation that the level of harmonisation of substantive and procedural law and the application of the principle of mutual recognition achieved so far was not sufficient to effectively combat crimes against the EU's financial interests.

Member States soon recognised that national action against EU subsidy and VAT fraud was ineffective, so the legislative will to set up a single prosecutor's office was there from the 1990s, but the Member States lacked the political will, and the EU lacked the necessary powers, so "only" the EU Anti-Fraud Office (OLAF) was established. The Lisbon Treaty of 2009 explicitly provided the possibility of establishing the EPPO, but the new treaty did not automatically create the organisation when it entered into force. However, Article 86 of the Treaty on the Functioning of the European Union (TFEU) required the unanimous support of the European Council (EC) and a majority of the European Parliament (EP). The authors of the Lisbon Treaty were prepared for a lack of consensus: in the absence of a full compromise, Article 329 TFEU opened the prospect of *enhanced cooperation* for determined Member States.[3] Enhanced cooperation[4] is a procedure under which at least 9 EU Member States are allowed to establish enhanced integration or cooperation within the EU in a specific area if it is established that the objectives of such cooperation cannot be achieved by the Union as a whole within a reasonable timeframe.

Article 86 TFEU therefore provides the legal basis for the establishment of a European Public Prosecutor's Office ¬ a technical implementation of Article 329 TFEU ¬ to investigate, prosecute and bring to justice the perpetrators and accessories to crimes against the Union's

[2] Mireille Delmas-Marty: The necessity, legitimacy and feasibility of Corpus Juris. Hungarian Law, 2000/11, pp. 641-645; Mireille Delmas-Marty -John A. E. Vervaele (eds.): The Implementation of the Corpus Juris in the Member States. Vol. Intersentia Publishing, Antwerp-Groningen-Oxford, 2000, pp. 7-394; Gabriele Dona: Towards a European Judicial Area? European Journal of Crime, Criminal Law and Criminal Justice, Vol.6/3, 1998, pp. 282-297; Ákos Farkas: Criminal Law Cooperation in the European Union. Osiris Publishing House, Budapest, 2001, pp.

[3] Szabolcs Petrus: Másfél éves az Európai Ügyészség – Érvek és ellenérvek tükrében 2023. Másfél éves az Európai Ügyészség – Érvek és ellenérvek tükrében – Jogászvilág

[4] Article 20 of the Treaty on European Union and Title III of the Treaty on the Functioning of the EU

financial interests. he European Public Prosecutor's Office is required to respect the principles of rule of law and proportionality in all its activities. The EPPO has to conduct its investigations in an impartial manner.[5] However, Article 86 of the TFEU does not contain a catalogue of offences falling within the remit of the EPPO, but merely declares that the EPPO can be "established for the purpose of prosecuting offences affecting the financial interests of the EU". In this context, it should be noted that the Court of Justice of the European Union (CJEU), in its judgment C-465/10[6] , confirmed the strict and broad interpretation of the protection of EU funds, even in cases where the offence is not a strict criminal offence but an administrative offence (e.g. a breach of public procurement rules). The importance of the decision lies in the fact that it has broadened the scope of the protection of financial interests by providing that a breach of public procurement rules, even if it does not directly involve fraud or a criminal offence, constitutes a breach of rules which is detrimental to the EU's financial interests. This broader interpretation has widened the scope for the possibility of recovering subsidies. On the other hand, the decision stressed that in the event of illegal use of Community funds, EU funds are subject to recovery in order to protect the EU's financial interests and must be dealt with under the limitation rules of Regulation (EC) No 2988/95. Thirdly, the decision paved the way for the future application of the PIF Directive[7] by providing a basis for its interpretation.

## 3. The EPPO's competences

### 3.1. The financial interest(s) [8] of the Union as a phenomenon and a protected legal subject

A key concept underpinning the operation of the EPPO is the notion of the "financial interests of the European Union." Although this concept has been defined in various ways from differing perspectives, all interpretations converge on the understanding that it refers to collective interests relating to the EU budget and the associated financial resources, revenues, and expenditures. These interests are intended to safeguard the economic stability and operational capacity of the European Union, as well as to ensure the lawful, efficient, and effective use of EU funds. The protection of the EU's financial interests is enshrined in Article 325 of the TFEU,

[5] Bence Udvarhelyi: The European Public Prosecutor's Office - from myth to reality. European Integration Studies, 15(1), 131-144. 2019. https://ojs.uni-miskolc.hu/index.php/eis/article/view/920.

[6] ECLI:EU:C:2011:867 CURIA - Documents

[7] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on combating crime against the financial interests of the European Union by means of criminal law (PIF Directive), OJ L 198, 28.7.2017, pp. 29-41.

[8] Corpus Juris introducing criminal law provisions in the financial interests of the European Union. Paris, Economica, 1997. Mireille Delmas-Marty - John A. E. Vervaele (eds.): Implementation of Corpus Juris in the Member States. Antwerp-Groningen-Oxford, Intersentia, 2000.

which states: *"The Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union."* The core elements of the EU's financial interests include, inter alia, the protection of revenue sources such as customs duties and VAT-based own resources. Equally important is the regularity and proper use of EU expenditure, including agricultural subsidies, cohesion funds, and research grants. These elements are critical to ensuring that EU resources are allocated and utilised in a manner consistent with the principles of legality, proportionality and financial management.

*Based on Euratom*

According to the definition provided in Council Regulation (EC, Euratom) No 2988/95[9] any act or omission that adversely affects the European Union's budget—on either the revenue or expenditure side—constitutes a breach of the Union's financial interests. Such conduct may occur intentionally (e.g., fraud), through negligence or via irregular procedures (e.g., violation of public procurement rules).

*According to the OLAF Directive*

The concept of the Union's financial interests is defined in Article 2(1) of Regulation (EU) No 883/2013[10] governing the operation of OLAF as "revenue, expenditure and assets of the European Union, the budgets of the institutions, bodies, offices and agencies and the budgets managed and controlled by them."

*According to the PIF Directive*[11]

The PIF Directive, in Article 2, clearly defines the concept of EU financial interests as all revenue, expenditure and assets financed, accruing from or due to the budget of the Union or the budgets of the Union institutions, bodies, offices and agencies established under the Treaties or budgets managed or controlled directly or indirectly by them. The PIF Directive will substantially increase the level of protection of the EU budget by harmonising the definitions, penalties and limitation periods for criminal offences against the financial interests of the Union. The Directive is a major milestone, but its legal basis has been the subject of several

[9] Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities' financial interests OJ L 312, 23.12.1995, p. 1-4 Regulation - 2988/95 - EN - EUR-Lex

[10] Regulation - 883/2013 - EN - EUR-Lex

[11] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on combating fraud affecting the financial interests of the Union by criminal law OJ L 198, 28.7.2017, p. 29-41 Directive - 2017/1371 - EN - EUR-Lex

debates during the legislative process and in the process of accession to the EPPO, as the arguments put forward by the Member States have been challenged.

This is one of the major difficulties in the functioning of the EPPO, which has been pointed out by several experts, including Burkhard Jähnke, former Vice-President of the German Federal Supreme Court and professor at Friedrich-Schiller-Universität Jena. According to him, the PIF Directive contains the most important substantive rules for the EPPO, but as it is a directive which is only binding in its purpose, and the Member States have not (necessarily) transposed it uniformly - the directive is supposed to give them room for manoeuvre - the EPPO is forced to apply dozens of substantive laws in cases with similar facts.[12] In agreement with the criticism, it is also worth pointing out that, although Member States had a strict deadline for implementing the PIF Directive, Romania, for example, has not yet complied with its obligation[13] to do so, and although Ireland and Denmark have *opt-in - opt-out* clauses, so it is acceptable for them to have done so, even these two countries have not transposed the Directive into their domestic legal systems. Interestingly, Poland, like Hungary, has not joined the EPPO but is in the process of transposing the PIF Directive.[14]

3.2. Offences within the scope of EPPO

Offences falling within the jurisdiction of the EPPO can be divided into three categories:[15]

*Firstly,* it has jurisdiction over so-called PIF offences under the PIF Directive, i.e. offences against the EU's financial interests as defined in the PIF Directive as transposed into national law, irrespective of whether the conduct in question a different type of offence under national law is also. It means that the competence of the EPPO covers the criminal offences defined in the PIF Directive, i.e. fraud affecting the Union's financial interests, money laundering, active and passive corruption and misappropriation, irrespective of whether the same criminal conduct could be classified as another type of offence under national law.[16]

The scope of the Directive clearly extends to own resources based on value added tax (VAT), but only applies to serious offences against the common VAT system, i.e. where the offence is linked to the territory of two or more Member States of the Union and causes total damage of

[12] Burkhard Jähnke, The principle of legality: a maxim of common European criminal procedural law, in Hefendehl, Hoyer, Rotsch, Schünemann (eds.), Journal of International Criminal Law. No. 5/12, p. 1 (3).
[13] see more in Rosalia Sicurella: The EPPO's material scope of competence and non-conformity of national implementations New Journal of European Criminal Law Volume 14, Issue 1. 2023.
[14] European Judicial Network (EJN)
[15] Petrus Szabolcs: i.m.
[16] Bence Udvarhelyi: i.m.

at least EUR 10 000 000. In my view, the scope of the Directive should cover all VAT fraud where it 'reduces Member States' tax revenue and thereby hinders the application of the uniform rate of VAT applicable to the VAT base of the Member States', as confirmed by the case law of the CJEU. According to which there is thus a direct link between, on the one hand, the collection of VAT revenue in the light of the applicable Community law and, on the other, the making available to the Community budget of the relevant VAT own resource, since failure to collect the former potentially leads to a reduction in the latter'.[17] However, the scope of the Directive is limited to cross-border VAT fraud where the above threshold is reached. In summary, the Directive refers *to fraud affecting the EU's financial interests*, which is mainly committed by the provision of false information, the concealment of information or the fraudulent use of aid or the fraudulent non-payment of aid, in relation to public procurement expenditure and value added tax (VAT, i.e. mainly VAT receipts).[18] In addition, Member States should also criminalise passive and active bribery, misappropriation and money laundering linked to fraud affecting the EU's financial interests.[19] Attempts to commit any of these offences should also be punishable.[20]

*Secondly,* the EPPO also has jurisdiction over offences relating to participation in a criminal organisation[21] if the criminal activities of such a criminal organisation are centred on the commission of any of the offences affecting the financial interests of the European Union.

*Thirdly,* the EPPO's jurisdiction also extends to any other offences that are inextricably linked to the aforementioned offences against the financial interests of the Union. Provided that the most severe penalty for the offence is not less severe than the penalty for the misdemeanour falling within the original jurisdiction of the *EPPO*.[22] The latter category of offences gives the EPPO the greatest margin of manoeuvre as regards its jurisdiction.

### 3.2.1 VAT fraud, VAT fraud, Member State contributions

The European Union has stressed the importance of the problem of tax fraud, particularly VAT fraud, in numerous documents, which is undeniable but overstated. The extension of the scope of the PIF Directive to VAT fraud was a significant step, in which the above-mentioned

[17]ECLI:EU:C:2011:733. European Commission v Federal Republic of Germany, paragraph 72.
[18] Article 3 PIF Directive (2017/1371)
[19] Article 4 PIF Directive (2017/1371)
[20] Article 5 PIF Directive (2017/1371)
[21] See: Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime [OJ L 300, 11.11.2008, p. 42-45].
[22] Article 25(3). EPPO Regulation (2017/1939)

interpretation of the CJEU was of crucial importance. Despite the cross-border dimension of the offence, this decision is still not without controversy, since VAT fraud directly affects the financial interests of individual Member States and only indirectly harms the financial interests of the Union, which is why the decision was taken to adopt a restrictive regulation based on value added.

### 3.2.2. Carousel fraud

At the same time, pragmatically, the EPPO Regulation also introduces limitations on jurisdiction. In the case of fraudulent schemes involving VAT-based own resources revenue - so-called carousel fraud - the Public Prosecutor's Office has jurisdiction only if the offence, contrary to the general territorial scope provision, is linked to the territory of two or more Member States of the Union and causes total damage of at least EUR 10 million (approximately HUF 3.1 billion). On the other hand, the Regulation establishes a categorical prohibition on offences relating to and inextricably linked to direct national taxation: these are in any case not covered by the European Public Prosecutor's Office. This rule is clearly intended to ensure that budgetary fraud hitherto investigated at national level does not swamp the Public Prosecutor's Office.[23] The practical difficulty of the latter is that, in criminal prosecution of the offence, the self-reporting ("Selbtstanzeige") is a criminal offence in some Member States (e.g. Germany and Austria), while in others it is not a legal instrument. In Hungary, there is the possibility of unlimited reduction of the penalty if the financial loss caused by the fiscal fraud is compensated before the charge is brought.[24] With regard to carousel fraud, the definition of "total loss" is a practical difficulty, as the preamble to the Directive defines "total loss" as the estimated amount of damage caused by the fraudulent scheme as a whole to the financial interests of the Member States concerned on the one hand and the Union on the other, but does not include interest rates and penalties. This solution of the Directive is the result of a political compromise, the consequences of which are suffered by the practitioners.[25]

---

[23] Ádám Békés - Tamás Gépész: Az Európai Ügyészség hatásköri szabályozása. Hatékony-e a köztes megoldás? Iustum Aequum Salutare XV. 2019. 2. 39-49. p.

[24] Pursuant to Article 396(8) of Act C of 2012 on the Criminal Code, the sentence of a person who compensates the pecuniary loss caused by the budget fraud as defined in paragraphs (1) to (6) before the indictment may be reduced without limit. This provision shall not apply if the offence is committed in a criminal conspiracy, criminal organisation or as a special repeat offender.

[25] Jancsa-Pék, Judit (2019) Az Európai Unió és a nemzeti hozzáadottértékadó-rendszerek kapcsolata. In: Harminckét lap, amely megrengette a világot: Százéves a hozzáadottérték-adó rendszere. Soproni Egyetem Kiadó, Sopron, pp. 269-398. ISBN 978-963-334-337-1; 978-963-334-337-1; Szabó Barna: A karusszel típusú csalások elleni küzdelem fegyvernemei és azok küzdelem fegyvernemei és azok célpontjai Magyar Rendészet 2020/1. 179—189. DOI: 10.32577/mr.2020.1.11

3.2.3. Corruption offences

Like money laundering, corruption is one of the offences that can be subject to criminal law harmonisation under Article 83(1) TFEU[26] . Bribery, which in many cases may be linked to fraudulent conduct, represents a very serious threat to the financial interests of the Union. Recognising this, the PIF Directive also regulates this offence, defining the offences of active and passive bribery and the range of sanctions applicable. The PIF Directive's definition of official covers all relevant officials, whether holding an official position in the Union, in Member States or in third countries. However, I believe that the increasing involvement of private individuals in the management of EU funds is a challenge and that, in order to ensure adequate protection of EU funds against bribery and misappropriation, the concept of official should also cover any person, such as contractors involved in the management of EU funds, who, although not holding an official position, performs a public task in relation to EU funds in a similar way, on the basis of a mandate. The EU should also develop effective rules to protect whistleblowers.[27]

3.3. Extending the scope - increasing efficiency or exercising stealth powers? Possible new offences within the EPPO's jurisdiction.

Although the European Public Prosecutor's Office is primarily intended to combat crimes affecting the financial interests of the European Union, Article 86(4) TFEU gives the European Council the possibility to extend the European Public Prosecutor's powers to other serious crimes with a cross-border dimension.[28]

The PIF Directive[29] has come in for much criticism because it introduces only minimal harmonisation of the relevant facts, meaning that even if fully implemented, it is likely that substantive criminal law provisions will remain fragmented and differ between Member States. The early fears and, in some cases, criticisms in this respect appear to have been confirmed once the EPPO has become operational, thus jeopardising the effectiveness of the Prosecutor's Office's work, as it will lead to the Prosecutor's Office having to deal with a whole variety of

[26] Read more by Laura Mickevičiūtė: Is there the Need for Further Harmonisation on Corruption Offences in the European Union? Kaiafa-Gbandi, M. (2010). Punishing Corruption in the Public and the Private Sector: The Legal Framework of the European Union in the International Scene and the Greek Legal Order, European Journal of Crime, Criminal Law and Criminal Justice, 18: 139-183.

[27] Márton Balázs: Az Európai Ügyészség, mint magyar nyomozó hatóság? (2023). Belügyi Szemle, 71(2), 287-302. https://doi.org/10.38146/BSZ.2023.2.6

[28] Bence Udvarhelyi: i.m.

[29] See, inter alia, John A. E. Vervaele: The material scope of competence of the European Public Prosecutor's Office, ERA Forum, vol. 15., no. 1. (2014) 97; Rosaria Sicurella: The European Public Prosecutor's Office and National Authorities. Milan, Wolters Kluwer-CEDAM, 124.

substantive criminal law rules.[30] At the same time, it should be borne in mind that the EPPO will only become operational in 2021, so that only 4 years of experience and indicators of operational functioning are available. In view of the above, it is, in my view, difficult to assess the current effectiveness of EPPO. The question is really whether the EPPO is ineffective in general or whether it is ineffective because, under the current regime, it does not have the scope to deal with the types of crime where it can and should be effective.

It is precisely because of this double ambivalence that the issue of the extension of the EPPO's powers is like a coin with two sides, so divisive between Member States and EU bodies and practitioners in the field. The critical view is that the functioning of the EPPO is chaotic even under the current jurisdictional arrangements, and the pro-sovereignty critics argue that an extension of its powers would result in nothing more than a continuation of the EU's stealthy expansion of powers. The '*forum shopping*' phenomenon is still unresolved and problematic, opening up a spiral of further concerns about the violation of the principle of *nullum crimen sine lege*, the rights of the defence and the principle of legality, among other burdens, and raising questions about the justification and necessity of extending the powers of a body that is already operating in a controversial manner.

On the contrary, based on an optimistic view, there may be several areas where the EPPO's remit could be extended. Such an ambitious objective can be justified and explained mainly for two main reasons. Firstly, the European Public Prosecutor's Office has demonstrated, on the basis of four years of concrete experience in the field of investigations, in the exercise of the powers currently conferred on it, that it has a particularly rapid and in-depth investigative capacity and all the necessary means to respond (albeit not without difficulty) to the huge volume of fraud and irregularities which are damaging European finances. Secondly, the establishment of a single European Public Prosecutor's Office will bring the integration of criminal justice to a much higher level than any other mechanism that has been in place so far, as it will have greater flexibility and speed than individual national prosecutors' offices.[31]

However the essential question remains, which new crimes the EPPO should investigate and prosecute. As a starting point, the question arises as to whether the extension should only cover cross-border offences defined as so-called 'euro crimes'. While another approach is to rely on a broader list of offences defined in instruments on mutual recognition of judicial decisions in

[30] Burkhard Jähnke i.m.

[31] Benedette Minucci: Towards an Expansion of EPPO's competences? in EUWEB Legal Esseays. Global & International Perspectives 2024. pp. 133-143.

criminal matters which are exempt from double criminality assessment, such as Article 2(2) of the Council Framework Decision on the European arrest warrant excluding double criminality. However, diverging views suggest that the ideal would be to include other offences with a typically cross-border dimension, such as market abuse and/or competition law infringements, in addition to these standards.[32]

One of these areas is eco-crime[33] , as sustainability and climate protection are becoming increasingly important in the EU. Illegal waste shipments are also currently a challenge for European criminal cooperation, as is the intentional damage to the environment and the deliberate circumvention of nature conservation legislation. Independently of this development, parallels can be observed between environmental crime and PIF crime. Both are serious crimes, often with a cross-border dimension; like PIF crime, environmental crime does not appear to be a priority for the national authorities of the Member States. Both areas of crime are 'victimless' and the environment, like the EU budget, is considered a 'European asset', and in both areas there is a residual footprint - eco or digital. Another similar area is drug trafficking and arms trafficking, both of which are quite 'lucrative' from the perpetrators' point of view, while the EU, on the other hand, is critically damaging to the budget.

The most urgent and pressing area, in my view, is the extension of powers *to cybercrime*, which is justified by the rapidly changing criminal environment. Cyberspace, including the open internet, also the deep and darkweb, transcends national borders and is not limited by the territorial jurisdiction of individual states. Investigating and prosecuting cybercrime therefore requires a common approach and a coherent strategy to enhance the security of the EU area.[34] Cybercrime is a global phenomenon and a growing threat in the areas of money laundering, corruption and VAT fraud. The old legislation developed before the digital age does not provide adequate tools to fight cybercrime, given that cybercrime is cross-border and investigation at national level is difficult. Attacks against EU infrastructures are still a critical area, and financial fraud and attacks against EU financial systems are a greater challenge, which is why the EPPO should not investigate these as related crimes, but as a separate offence under a separate jurisdiction rule. Given the specific location of cybercrimes and the forensic and technical challenges of investigation, it would be advantageous to include all forms of cybercrime under

[32] Prof. Dr. Mar Jimeno Bulnes: The European Public Prosecutor's Office and Environmental Crime Further Competence in the Near Future? Eucrim Issue 2/2024. pp. 146-152.

[33] see more in The European Public Prosecutor's Office and Environmental Crime - eucrim

[34] Viz. Zarychta-Romanowska, K. Creating an EU "Homeland Security". In Scott, N. R., Kaunert, Ch., Fabe, A. P. H. (ed.) Countering Terrorist and Criminal Financing: Theory and Practice, Boca Raton: CRC Press, 2023.

the jurisdiction of the EPPO. Firstly, there would be a clear benefit in having the EPPO at the centre of a dense international cooperation network, dealing with complex challenges and managing investigations that may go beyond the individual capabilities of Member States. European Delegated Prosecutors operate in the context of a 'dual legal track', integrating into the legal systems of the Member States while cooperating effectively with Eurojust and Europol. In contrast to the approach of national prosecutors, the EPPO's involvement can facilitate direct contacts between the authorities of the Member States concerned and other bodies.[35] Secondly, it should not be overlooked that the EPPO's ability to ensure timely and comprehensive exchange of information [...] would therefore facilitate the flow of information within the Union, allowing for a rapid and targeted response to transnational crime.

Considerations for extending the EPPO's jurisdiction are naturally motivated by the interest in protecting fundamental social goods and values. In accordance with the principle of subsidiarity, the EU is entitled to act when the desired objectives cannot be sufficiently achieved by the Member States.[36]

## 4. The role of the EPPO in criminal cooperation against cybercrime

### 4.1. The EPPO as a victim of cybercrime?

As a "side effect" of the rapid digitalisation of finance, cybercrime has exploded.[37] The European Union is not only a regulatory and enforcement actor in cyberspace, but is also increasingly a target, especially in financial and institutional terms. The EU institutions, agencies and programmes are regularly the victims of cyber-attacks, phishing campaigns, 'whaling' and digital fraud and ransomware attacks, which directly threaten the EU's financial interests[38], and the draft introduction of the digital euro is still in its early stages.

The EU allocates hundreds of billions of euros to different national, regional and thematic objectives through structural and investment funds. EU funding schemes (e.g. the Recovery and Resilience Instrument, Horizon Europe, Cohesion Funds) are particularly vulnerable to

[35] Benedetta Minucci: i.m.
[36] Bianka Bilasová and Štěpán Kořínek: The European Public Prosecutor's Office in the fight against Cybercrimes in International Conference on Social and Healthcare Studies 72-87. pp.
[37] Levente Kovács - Elemér Terták: A kiberbűnözés legjobb ellenszere a pénzügyi műveltség Gazdaság és pénzügy 11. évfolyam 1. szám (2024) DOI: 10.33926/GP.2024.1.2
[38] Directive (EU) 2017/1371 of the European Parliament and of the Council, recital (1): the primary role of the protection of the Union's financial interests.

attempts to circumvent them through cyber-attacks or digitally-enabled fraud[39] . These attacks can be aimed at, for example, misappropriating grant funds, manipulating project documentation or falsifying procurement data. In such cases, the EU becomes an injured party, which justifies action by Member States and, where appropriate, the EPPO.[40]The number of attacks of this type is on the rise, as confirmed by annual reports from Europol and ENISA (European Cybersecurity Agency)[41] . Victimisation of the EU can result not only in financial loss but also in a loss of institutional confidence and weakened enforcement of the rule of law, especially in digitally vulnerable Member States.

*Reasons for exposure to cybercrime*

*First of all,* the vulnerability of digital systems is a real risk factor for cybercrime. EU tenders are submitted, evaluated and checked in electronic systems such as SFC2021, TENtec, Funding & Tenders Portal. These platforms are used to perform administrative tasks related to EU research, innovation and other funding programmes, including accessing, submitting and managing proposals, and therefore handle a mass of very sensitive financial and personal data, which makes them an opportunity for a number of cybercrimes if the appropriate security measures are missing or can be circumvented. These systems can also be the target of phishing attacks to obtain login details (EU Login username/password) via fraudulent emails or websites, which pose a significant risk of unauthorised access to applications, financial documents and thus manipulation, withdrawal or submission of false data. On the other hand, they can also be targets of a breach of the system, which could result in the manipulation of financial transactions or decision data. At the same time, it is an important distinction that denial of service attacks (DDoS) against the system, which are aimed at preventing the functioning of the portal, are not necessarily committed for financial gain but to distort competition or for political purposes, which is why it would be appropriate to extend the EPPO's jurisdiction to all cybercrimes, as the intent, motive and result may differ for the elements of a series of attacks.

*Secondly*, there is a serious risk of manipulation of payment systems, which could cause damage to the financial interests of the European Union (and thus make the EPPO relevant) that is much more significant than the scope of the attacks mentioned above. Payment systems play an

[39]European Court of Auditors, *Special Report 13/2022*: "Fighting fraud in EU spending: action needed", in particular the risks of digital attacks on EU funds.
[40] Council Regulation (EU) 2017/1939, Article 4 and Article 24(1): the EPPO is empowered to act in cases of criminal offences affecting the financial interests of the Union, the EU is in a victim's position.
[41] Europol: *Internet Organised Crime Threat Assessment (IOCTA) 2023* and ENISA: *Threat Landscape Report 2023*.

important role in the implementation of the EU budget, as a large part of EU funds are paid under shared management, in which the Commission and Member States participate jointly. When subsidies are paid, they work with banking data, with contracts, with invoices, which are susceptible to falsification. A common modus operandi is to enter false beneficiary bank account numbers, upload false financial documentation or modify payment claims by accessing the system, thereby committing crimes to the detriment of the EU budget.

The financial interests of the European Union cover both the revenue and expenditure sides of the EU budget. Under the PIF Directive, the financial interest is affected when EU funds are wrongly granted, paid or used as a result of illegal activities. According to Article 3 of the PIF Directive, the following types of conduct are considered to be contrary to the EU's financial interests:

- misappropriation, illegal acquisition which shall be understood as expenditure based on false or fraudulent statements made in order to obtain the right,
- misappropriation, illegal use, which is defined as use other than for the intended purpose and which is or is likely to be detrimental to the EU budget,
- Unlawful retention, which is the withholding of funds which are unlawfully retained.

4.2. Cybercrimes within the jurisdiction of the EPPO

The EPPO was established specifically to protect the financial interests of the European Union, *de facto* to protect funds effectively. Its task is to investigate, prosecute and bring to justice crimes that harm the EU's financial interests. These include many types of fraud, VAT fraud involving more than €10 million, money laundering, corruption, etc. The EPPO investigates, prosecutes and acts as a prosecutor in the competent courts of the participating Member States until the case is finally closed. Until the EPPO became operational, only national authorities could investigate and prosecute these offences, but their jurisdiction stopped at their national borders. Organisations such as Eurojust, OLAF and Europol do not have the necessary powers to prosecute. Modern forms of crime such as cybercrime present new challenges for law enforcement authorities, including prosecutors. One new challenge is to address aspects of cybercrime. This raises the question of *what possibilities does the EPPO have to investigate and prosecute cybercrime*?

The EPPO's jurisdiction is essentially limited to crimes against the financial interests of the European Union, as defined in the PIF Directive. Consequently, cybercrimes per se do not automatically fall within the jurisdiction of the EPPO. However, where the cybercrime directly

or indirectly affects the EU's financial interests, the EPPO may have jurisdiction to prosecute. This could include, for example, cyber fraud involving EU funds (e.g. creating fake websites to divert funds), digital VAT fraud, in particular in cross-border e-commerce, where the damage caused exceeds €10 million, and money laundering involving EU funds when it takes place through digital transactions. The EPPO therefore has jurisdiction over cybercrime only if the act is financially closely linked to or facilitates the commission of a crime involving the EU budget. General cybercrime (e.g. ransomware, theft of personal data from state systems) will remain within the jurisdiction of national investigative authorities. Thus, if a hacker attacks a national health database, it is not within the EPPO's jurisdiction, but if a criminal organisation uses a fake billing system to defraud EU funding, it could be EPPO jurisdiction. Cyberspace transcends national borders and is not limited by the territorial jurisdiction of individual states. Investigating and prosecuting cybercrime therefore requires a common approach and a coherent strategy that would enhance the security of the EU area. The role of the European Public Prosecutor's Office in combating payment fraud, such as credit card fraud and online money laundering, is limited, although this type of crime is on the rise. The rise of the digital space is accompanied by a multiplication of cyber fraud. The most common cases include, for example, the misappropriation of EU funds from an IT service provider on the basis of false consultancy invoices.

In the case of computer crime, or more precisely, cybercrime must be understood in a broader context, which includes *cyberterrorism*. Cyberterrorism can be defined as the use or misuse of information and communication technologies for terrorist activities by actors to achieve their terrorist goals. It can include activities such as propaganda, financing, training, planning, execution and ultimately the terrorist attacks themselves. From a doctrinal point of view, although there are many different definitions of cyberterrorism, all should highlight the convergence of terrorism and cyberspace. This raises the question: *why should the EPPO's competencies be extended to cybercrime, in concreto cyberterrorism?* Terrorism has an impact on the fundamental values on which the EU is built, and it is therefore essential to protect them. In the modern era, cybercrime or cyberterrorism have the potential to cause significant negative consequences, such as disruption of telecommunications, energy, industrial, economic and transport infrastructure and financial damage. Addressing cybercrime requires close interstate cooperation to effectively maximize protection. Terrorist groups regularly use cyberspace, typically for online radicalisation, to intimidate as many users as possible by distributing provocative videos. Such activities lack the element of physical presence at the site of the attack,

but technically leave traces, i.e. *digital footprints*. As with 'traditional' forms of crime, cybercrime (including cyberterrorism) has a number of psychological aspects, both for the perpetrators and the victims.[42] The use of the Internet allows investigative agencies to follow digital trails and subsequently gather information that facilitates the prosecution of the perpetrators of such illegal activities.[43] Assuming that jurisdiction to deal with serious cybercrime is transferred to the EPPO, the risk of jurisdictional conflict would be eliminated[44]. . Currently, there can be situations where two states claim jurisdiction over a particular crime with a cross-border element. This conflict of jurisdiction could lead to a violation of individuals' fundamental rights and freedoms, for instance, by violating the *ne bis in idem principle.* Moreover, the volatility of the digital environment requires a very rapid exchange of information and the provision of evidence, in particular electronic evidence (e-evidence). However, traditional instruments of legal aid in international judicial cooperation are not designed for the digital age. Even some of the more modern instruments, such as the European Investigation Order, no longer seem adequate.[45]

4.3. EPPO action against cybercrime affecting financial interests

The current legislative framework, based on the EPPO regulation, stipulates that the European Public Prosecutor is authorised to conduct investigative actions such as inspecting computer systems and securing data contained therein. The EPPO investigates what are known as 'euro-crimes'. *De facto* the most common offence involves the illegal activity of the submission of false, incorrect or incomplete information during a public procurement procedure, leading to misappropriation or wrongful withholding of funds. The EPPO is also responsible for prosecuting the misuse of funds from the EU budget. Data theft or data leakage in relation to EU tenders, leading to false grant applications, is becoming increasingly common; manipulation of payment systems by altering bank account details as detailed above through phishing or malware.[46] Also common is the falsification of electronic documents and digital accounts; and unauthorised access to EU platforms (e.g. Funding & Tenders Portal, SFC2021);

[42] Prince, J. Psychological Aspects of Cyber Hate and Cyber Terrorism, in Awan, I., Blakemore, B. Policing Cyber Hate, Cyber Threats and Cyber Terrorism, Farnham: Ashgate, 2012, p. 21-38.

[43] Bianka Bilasová and Štěpán Kořínek: i.m. p. 79.

[44] The author's position can and in my view, should be challenged, as the main criticism of the EPPO is that forum shopping goes hand in hand with jurisdictional issues.

[45] Bianka Bilasová and Štěpán Kořínek i.m. 80.p.

[46] Malware is an umbrella term, encompassing all kinds of malicious software, including the most well-known types such as Trojans, ransomware, viruses, worms and banking malware.

and digital money laundering, for example through the laundering of EU funds via cryptocurrency.

From the above it is clear that the EPPO's competence does not automatically include the adjudication of cybercrime cases and although it does not exclusively deal with cybercrime, these cases are increasingly part of the EPPO's portfolio. The falsification of electronic documents and digital accounts; and unauthorised access to EU platforms (e.g. Funding & Tenders Portal, SFC2021) are also common; and digital money laundering, for example by laundering EU funds through cryptocurrency, is becoming more and more prevalent. *Pro futuro* the EPPO could have the authority to prosecute terrorist crimes, such as terrorist financing.

The EPPO's action can be based on a complaint or *ex officio* if it detects an anomaly through automatic data linking, which can be based for example on recommendations made by OLAF in a prior procedure or on the digital monitoring activities of a national authority in a Member State. The EPPO's procedural powers range from seizure of cyber assets, to gathering digital evidence, to coordinating national investigations. The novelty of these procedural prerogatives, compared to other EU law enforcement bodies, is the prosecutorial power, so the EPPO prosecutes cybercrimes against the financial interests of the Union and acts as a prosecutor in trials before national courts. The EPPO collects data from tender systems, emails, billing chains and digital evidence as part of a preliminary investigation. Taking into account the speciality of the place of offence, which is cyberspace, this is done on servers or, in the case of files stored in a cloud environment, on cloud-based storage, using IP addresses, hashes, metadata. Or, using the acquis of cross-border criminal cooperation such as the European arrest warrant (EAW), European investigation order (EIO) or freezing order. EPPO prosecutors can take action simultaneously in several Member States to carry out investigative measures (e.g. search and seizure, witness hearings). Although the EIO is a versatile instrument for judicial cooperation applicable to a wide range of evidence, it appears to be insufficient for electronic evidence, which urgently needs to be addressed and to which the EU must respond within a short timeframe. Perhaps a solution could be found in the electronic evidence instruments under the E-evidence Regulation, which is not yet fully developed.

The EPPO works closely with and is, in fact, reliant on cooperation with EC3, which operates within Europol, in the field of cybercrime. Despite the fact that EC3 does not have independent investigative powers, because criminal justice remains the responsibility of the Member States (as state criminal powers are the bulwark of their sovereignty), it is primarily through its coordination, analysis and support functions that it effectively tackles cybercrime. It has a

significant added value through its technological toolbox, its analytical capabilities and its international network. Its remit covers crimes against children in the online space (e.g. child pornography, online grooming, etc.), serious and organised cybercrime (e.g. ransomware, botnets), payment fraud (e.g. credit card fraud, online money laundering), darknet and cryptocurrency-based crime, and intelligence operations related to state-sponsored cyber-attacks. EC3 is at the forefront in terms of technological tools and intelligence infrastructure, given its ability to analyse anonymised networks (e.g. Tor) through its Darknet Monitoring Capability, and to provide tools for crypto-transaction tracking (Cryptocurrency Tracking Tools), as well as real-time internet monitoring capabilities (Cyber Patrol) and on-site and remote data processing and evidence validation through its Digital Forensics Lab. But malware can also be identified and classified using the Malware Analysis Platform.

## 5. Problem statements and proposed solutions

The way EPPO has worked so far has probably created more procedural problems than it has solved. From the problems of *forum shopping* – which could be the subject of another independent study – to the shortcomings in the transposition of the PIF Directive and the funding deficit, to the lack of redress and democratic oversight, the range of problems is quite wide. In my view, the biggest problem with the current operation of the EPPO, although young but by no means in its infancy, is the limited and fragmented nature of its powers. These affect not only its effectiveness, but also legal certainty and consistent law enforcement. On the one hand, the EPPO has limited material jurisdiction, as it only has jurisdiction over ’PIF offences’, but these are not the only offences that cause material damage to the EU budget and damage its financial interests. It cannot investigate money laundering, cybercrime or organised crime if they are not directly linked to EU funds, which in practice could create an operational barrier. As a given offence may involve several aspects (e.g. corruption and VAT fraud), but if the EPPO's jurisdiction only covers one part, a fragmented investigation may result. As a given offence may involve several aspects (e.g. corruption and VAT fraud), but if the EPPO's jurisdiction only covers one part, a fragmented investigation may result. In the former case, the defence aspect cannot be ignored, since while the prosecuting authority is an EU body, there is no EU advocacy, and therefore the balance of arms is significantly out of balance. At the same time, in line with the main thrust of the study, it is more important to highlight that the 'formal division of powers' with national prosecutors' offices can also lead to operational confusion. The distinction is not always clear, especially in mixed cases (e.g. involving both EU and national sources), in which case parallel investigations are launched or jurisdictional disputes

arise. It should also be mentioned that, although the EPPO is an EU body, there is no debate about a uniform EU criminal law, since the enforcement of state criminal law and national criminal law is the ultimate bastion of sovereignty under the internal law of each Member State, and therefore the EPPO must conduct all proceedings in accordance with the criminal law of the Member State concerned. While in theory, this should not be a problem, because in an ideal Union all Member States would comply uniformly with their implementation obligations, which would result in a uniform treatment, but the reality is different, with differences in procedural rights, assessment of evidence, interpretation of extended confiscation and reversal of the burden of proof, which makes uniform action difficult and creates legal uncertainty while at the same time all Member States face a sharp increase in cybercrime.

Despite these operational problems, according to *my hypothesis* the EPPO's jurisdiction should cover all cybercrimes. At present if a criminal organisation hacks into an EU agricultural support system and initiates an unauthorised payment, it is currently not certain that the case falls within the remit of the EPPO. At the moment, the prosecution of cybercrime remains very much a Member State competence, while fraud is tackled at EU level, which can lead to a legal loophole where the purpose of the crime committed by digital means is to obtain EU money. An extension of the EPPO's competence would remove this inconsistency. The cross-border nature of cybercrime is beyond dispute. Perpetrators, victims, servers and financial transactions can be linked to different countries, and national authorities can only act in their own jurisdiction - so investigations fall apart, often in an uncoordinated way. Setting up JITs can help somewhat in these cases. However, not all Member States have specialised IT investigators, tools and cyber intelligence systems, so the technical backlog of smaller or less developed states poses a risk for the EU as a whole, while the EPPO, with its digital forensic units and EU prosecution teams specialised in cybercrime, could respond more quickly to already time-sensitive crimes. Another argument against the Member State level is that international mutual legal assistance procedures (e.g. MLA or even the 24/7 networks established by the Budapest Convention) are very time-consuming and formalised, by the time one country responds to another, traces can disappear, cryptocurrency moves on, servers are wiped at the touch of a button, while the EPPO's internal information systems allow automatic data exchange, intelligent interconnections based on e.g. IP address, money movements, server locations.

The EU has already recognised the threat of cybercrime and has started to develop EU cyber defence strategies (e.g. NIS2 Directive, Cyber Solidarity Act), which include the involvement

of EPPO. In my view, extending the EPPO's competence to cybercrime is not only justified but also strategically necessary to protect the EU's financial, rule of law and security interests, but could only be done gradually, on a clear legal basis, with the will of Member States and adequate financial resources. At the same time, I would point out that this proposed solution can only be implemented gradually and with due caution. Cybercrime requires specific IT knowledge, digital assets and data protection protocols, which are currently not available. Thus, adding additional tasks could lead to a collapse unless there is a concomitant significant increase in resources. However, until such an extension of powers takes place, the EPPO will continue to use its existing powers and tools to tackle crimes against the financial interests of the Union, of which *asset recovery is* a key element. The EPPO's asset recovery activities are far from perfect and some concerns in this area - in particular the fundamental rights aspect of extended confiscation and the adequacy of the evidence of the right of appeal - are well founded.

## 6. Concluding thoughts

The EPPO has become a key actor in the protection of the EU's financial interests and the administration of justice. I share the view that one of its most important contributions lies in its independence from national influence, particularly in investigating and prosecuting serious criminal cases at EU level that would otherwise be subject to political pressure at national level.[47] Based on the empirical results of its operations to date, the EPPO can be regarded as a functioning and effective body, which, at least for the time being, clearly demonstrates added value in safeguarding the EU's financial interests. It has achieved a remarkable effectiveness in dealing with serious cross-border crime, which underlines the growing need for solid and effective cross-border cooperation, despite signs that mutual trust between Member States in each other's legal systems seems to be faltering in some cases. As regards the possible extension of the EPPO's powers, I believe that, in the case of serious organised crime and cybercrime, it would be an institutionally functional solution to increase the effectiveness of the prevention and punishment of these forms of crime. Cybercrime has become part of our everyday lives, affecting the financial interests of individual states and the European Union, with significant consequences, since economic interdependence between Member States is central to ensuring the continued development and stability of their economies. The financial interests of the EU

[47] For an opinion partly questioning and partly contradicting the political independence of the EPPO, see Balázs Márton, Independence of the European Public Prosecutor's Office in the context of the appointment procedures, New Journal of European Criminal Law, 15(2), 2024. 146-163. https://doi.org/10.1177/20322844241228721

are closely linked to those of the Member States and individuals, as they are functionally integrated in this common economic space.