

# eucrim

2025 /

1

European Law Forum: Prevention • Investigation • Prosecution



**Reform challenges in a reinforced Area of Freedom, Security and Justice**

**Les défis de la réforme dans un espace de liberté, de sécurité et de justice renforcé**

**Reformherausforderungen in einem verstärkten Raum der Freiheit, der Sicherheit und des Rechts**

Guest Editorial by *Vânia Costa Ramos*

*Elisa Sason, Cristina Monti and Pablo Olivares Martínez: Security – A Firm Construct or an Undetermined Concept?*

*Mirjana Jurić: The Role of an AFCOS in a New Anti-fraud Architecture*

*Georgia Theodorakakou and Luis Jakobi: Conference Report: Strengthening the Future of the EPPO*

*Kris Meskens and Julie Vanstappen: Le futur rôle des Cellules de Renseignement Financier*

*Claudia Cantisani and Laura Ricci: The Fight against Agri-Frauds*

*Francesco Lo Gerfo: Yellow Card Legislation and Infringements of Agricultural Aid Rules*

*Fabian M. Teichmann: Non-Conviction-Based Confiscation (NCBC) – A Reform Option for German Asset Recovery Law*

*Randall Stephenson, Johanna Rinceanu, and Marc André Bovermann: Regulating Political Advertising in the EU*

*Tinka Reichmann: Übersetzen und Dolmetschen im Rechtswesen*

euocrim also serves as a platform for the Associations for European Criminal Law and the Protection of Financial Interests of the EU – a network of academics and practitioners. The aim of this cooperation is to develop a European criminal law which both respects civil liberties and at the same time protects European citizens and the European institutions effectively. More information about the Associations is available at <https://euocrim.eu/associations/>.

# Contents

## News

### European Union

#### Foundations

- 2 Rule of Law
- 2 Area of Freedom, Security and Justice
- 3 Security Union
- 4 Schengen
- 6 Ukraine conflict
- 11 Artificial Intelligence (AI)
- 12 Digital Space Regulation

#### Institutions

- 14 Commission
- 15 Europol
- 16 Eurojust
- 17 Frontex
- 18 European Data Protection Supervisor (EDPS)
- 19 European Public Prosecutor's Office (EPPO)

#### Specific Areas of Crime

- 22 Protection of Financial Interests
- 24 Money Laundering
- 25 Tax Evasion
- 26 Counterfeiting & Piracy
- 27 Cybercrime
- 28 Organised Crime
- 29 Trafficking in Human Beings

#### Procedural Law

- 31 Procedural Safeguards
- 32 Data Protection
- 32 Ne bis in idem
- 33 Victim Protection
- 34 Freezing of Assets / Confiscation

#### Cooperation

- 34 Police Cooperation
- 35 Judicial Cooperation
- 36 European Arrest Warrant
- 37 Law Enforcement Cooperation

### Council of Europe

#### Foundations

- 37 Rule of Law
- 38 European Court of Human Rights

#### Specific Areas of Crime

- 39 Corruption
- 39 Money Laundering
- 40 Counterfeiting & Piracy
- 41 Terrorism

## Articles

### Reform Challenges in a Reinforced Area of Freedom, Security and Justice

- 42 Fil rouge  
*Lothar Kuhl*
- 43 Security – A Firm Construct or an Undetermined Concept? – An Outline of the EU's Current and Future Security Architecture  
*Elisa Sason, Cristina Monti, and Pablo Olivares Martínez*
- 53 The Role of an AFCOS in a New Anti-fraud Architecture  
*Mirjana Jurić*
- 57 Conference Report: Strengthening the Future of the EPPO  
*Theodorakakou and Luis Jakobi*
- 61 Le futur rôle des Cellules de Renseignement Financier  
*Kris Meskens and Julie Vanstappen*
- 72 The Fight against Agri-Frauds – Suggestions to Improve Cross-Border Cooperation  
*Claudia Cantisani and Laura Ricci*
- 77 Yellow Card Legislation and Infringements of Agricultural Aid Rules – A Case Study of a Regressive Penalty Structure  
*Francesco Lo Gerfo*
- 84 Non-Conviction-Based Confiscation (NCBC) – A Reform Option for German Asset Recovery Law  
*Fabian M. Teichmann*
- 90 Regulating Political Advertising in the EU – Transparency Without Accountability  
*Randall Stephenson, Johanna Rinceanu, and Marc André Bovermann*
- 97 Übersetzen und Dolmetschen im Rechtswesen  
*Tinka Reichmann*

# Guest Editorial

Dear Readers,

Over two decades have passed since the EU's first attempt to harmonise procedural rights in criminal proceedings across the bloc. The [2009 Roadmap](#), adopted under the Swedish Council Presidency, led to six key directives: on [interpretation and translation](#), [information rights](#), [access to a lawyer](#), [presumption of innocence](#) and the right to be present at trial, [safeguards for children](#), and [legal aid](#). Two recommendations followed, addressing [vulnerable persons](#) and [pre-trial detention conditions](#).

Yet, despite these advances, the EU still lacks a coherent and equal system of procedural rights. While the existing instruments might give the impression of a developing European code of criminal procedure, this is far from the reality. In practice, individuals and corporations continue to face significant disparities in legal protections depending on where they are investigated or prosecuted.

Basic elements remain fragmented. Just to give a few examples: whether a person whose assets are frozen may access case materials to contest the measure, and by what means; whether a lawyer can be present during a search; whether the accused is granted access to a copy of a seized device containing digital evidence; whether intercepted communications may be used in subsequent prosecutions; whether *hacking for evidence* is admissible; whether a poor person can choose their own lawyer; whether defence lawyers are permitted to conduct independent investigations; whether an accused person residing in another Members State may attend their trial remotely, etc.

The 2009 Lisbon Treaty expanded the EU's competence in the field of criminal justice, providing for minimum rules in areas such as mutual admissibility of evidence, the rights of individuals and victims, and other procedural aspects. It also laid the foundation for the creation of the European Public Prosecutor's Office (EPPO). Since then, the EU criminal justice landscape has evolved dramatically: the EPPO is now operational, mutual recognition instruments are widely used, and the mandates of both Europol and Eurojust have grown – with [further expansion under discussion](#).

In this context, claiming that no further EU action is needed is not only short-sighted but also undermines the Union's commitment to justice and fundamental rights. As [I have](#)

[previously stated](#): “There is no such equal and effective protection throughout the EU. Even well-established rights at national level become blurred in cross-border or EU-led prosecutions.” This legal uncertainty weakens both the protection of rights and the effectiveness of justice. It is no longer acceptable that individuals or companies can be subject to cross-border investigations – often led by EU bodies – without consistent procedural protections or access to EU-funded legal aid.



Vânia Costa Ramos

We urgently need a new generation of EU rules to address the following key areas:

- The [right to legal assistance and legal aid, including in cross-border cases](#);
- [Legal privilege and confidentiality](#);
- Safeguards for interception measures, especially those not tied to a specific territory;
- [Procedural rights concerning digital evidence](#);
- Access to the case file;
- [Remote participation in proceedings](#);
- [Pre-trial detention standards](#);
- [Effective remedies, including exclusionary rules for evidence obtained in violation of rights](#);
- [Harmonised safeguards in EPPO proceedings](#);
- [Mutual recognition of protective decisions such as extradition refusals](#);
- A meaningful right to judicial review before the CJEU, [particularly regarding EPPO acts](#).

We must move toward a truly European framework of defence rights – one that reflects the digital age, the transnational nature of crime, and the evolving role of EU institutions. The ongoing High-Level Forum on the Future of Criminal Justice is a unique opportunity to shape this vision. The EU must be bold and resolute in advancing the area of freedom, security, and justice. A [new roadmap](#) for procedural rights, adapted to today's realities and built to last, is not only necessary, but long overdue.

Vânia Costa Ramos

Lawyer, Chair of the European Criminal Bar Association (ECBA)



### European Union

Reported by Thomas Wahl (TW), Cornelia Riehle (CR), and Dr. Anna Pinggen (AP)

#### Foundations

##### Rule of Law

##### ECJ: Polish Judge Retains Jurisdiction after Unlawful Withdrawal of Cases

In its [judgment](#) of 6 March 2025 in Joined Cases [C-647/21 \(D.K.\)](#) and [C-648/21 \(M.C. and M.F.\)](#), the European Court of Justice (ECJ) clarified that the decision to withdraw cases from a judge is subject to objective and precise criteria and must always include a statement of reasons in order to rule out arbitrariness or disguised disciplinary penalties.

The trigger for this was the case of a Polish judge who, in 2021, had been removed from around 70 pending cases by the college of judges of a regional court without prior notice and justification. The cases were re-assigned to other judges instead. The judge, who had previously questioned, among other things, the legality of the appointment of another judge, received no explanation and was unable to seek judicial review of the measure. She herself referred two of these cas-

es, from which she was removed, to the ECJ for a preliminary ruling.

The ECJ emphasised that Art. 19(1), second subparagraph, TEU protects judicial independence not only from external influences, but also from internal influence by court administrations or collegial bodies. Rules that allow the withdrawal of cases without objective criteria and without justification compromise judicial independence. Such an interference can have the effect of a covert disciplinary measure or lead to a judge being put under pressure because of substantive rulings. Under EU law, national courts are obliged, by reason of the primacy of EU law, to disapply such measures and the reallocation of cases. The judge concerned must be able to continue to act in the proceedings submitted. (TW)

##### Area of Freedom, Security and Justice

##### ECJ Topples Malta's Golden Passport Scheme

The acquisition of Union citizenship cannot result from a commercial transaction. This was decided by the

ECJ in its [judgment](#) of 29 April 2025 ([Case C-181/23, Commission v Malta](#)). The Court ruled that the programme "Maltese Citizenship by Naturalisation for Exceptional Services by Direct Investment" is contrary to EU law.

Since 2020, Malta has allowed foreign investors to apply for Maltese citizenship (and thus, if granted, acquire automatically Union citizenship) if they meet certain requirements, mainly of a financial nature. The approach has often also been referred to as "golden passport scheme".

In response to an action for failure to fulfil obligations brought by the European Commission, the ECJ ruled that it is in principle for the Member States to determine the conditions for granting and losing nationality. However, this national competence must be exercised in accordance with EU law. The judges in Luxembourg emphasised that Union citizenship is one of the principal concrete expressions of the solidarity which forms the very basis of the integration process (the *raison d'être* of the EU itself). It is therefore an integral part of the identity of the EU as a specific legal system, accepted by the Member States on a basis of reciprocity. Moreover, in accordance with the principle of sincere cooperation enshrined in Art. 4(3) TEU, it is for each Member State to refrain from any measure which could jeopardise the attainment of the EU's objectives.

\* Unless stated otherwise, the news items in the following sections cover the period 16 January 2025 – 30 April 2025. Have a look at the eucrim website (<https://eucrim.eu>), too, where all news items have been published beforehand.

Accordingly, granting nationality in direct exchange for predetermined investments or payments through a transactional procedure manifestly infringes these EU values and the Court calls such “commercialisation” of citizenship being incompatible with the basic concept of Union citizenship as defined by the Treaties. Such a practice does not make it possible to establish the necessary bond of solidarity and good faith between a Member State and its citizens, or to ensure mutual trust between the Member States and thus constitutes a breach of the principle of sincere cooperation.

The European Commission has eyed the “golden passports” schemes for several years. Among other things, it fears that they could open the door to money laundering and corruption. Golden passports were also issued in Cyprus, among other places, but the government withdrew them under pressure from the Commission. (TW)

### EU-CLASI Joint Declaration on Internal Security

In the margins of the Home Affairs Council meeting on 5 March 2025, EU ministers of home affairs met with their counterparts of the Latin American Committee on Internal Security (CLASI). CLASI is currently composed of 16 Latin American countries and is the EU’s privileged partner to enhance law enforcement cooperation with Latin America and the Caribbean. It has been the third exchange at ministerial level since 2022 and 2023. The meeting focused on addressing common internal security threats, in particular as regards the fight against transnational serious and organised crime and illicit drug trafficking. EU and CLASI home affairs ministers agreed on a [joint declaration and a roadmap](#) to implement operational cooperation priorities in 2025–2026 (annexed to the joint declaration). The cooperation priorities include:

- Strengthen the exchange of infor-


mation between law enforcement in both regions;

- Strengthen the sharing of information regarding drug trafficking;
- Develop actions against the most threatening criminal networks;
- Enhance cooperation of CLASI countries with key EU agencies from the justice and home affairs area;
- Assess continuously the security vulnerabilities of ports of both regions and the measures put in place to counter the infiltration of organised crime;
- Promote the implementation of the “follow the money” approach, targeting the economic infrastructure of organised crime.

The home affairs ministers of the EU and CLASI also agreed on an 18-month cycle of meetings at ministerial, institutional and senior officials’ level. (TW)

### Security Union

#### Commission Presents ProtectEU: the New EU Internal Security Strategy

 On 1 April 2025, the European Commission [presented](#) a Communication entitled “[ProtectEU: a European Internal Security Strategy](#)”. The Strategy outlines a comprehensive set of measures that are planned to be initiated and implemented in the current term of the Commission in order to strengthen the EU’s internal security. The Strategy reacts to the changing security threat landscape, such as the blurring lines between hybrid threats and open warfare, more and more powerful organised crime networks spilling into EU’s economy, the continuous looming terrorist threat level in Europe, and the increasingly prevalent exploitation of new technologies for crimes. The Strategy aims at upgrading the Union’s capacity to anticipate, prevent and respond to the security threats.

It is guided by the following three principles:

- Changing the culture on security: a whole-of-society approach involving all citizens and stakeholders, including civil society, research, academia and private entities is envisaged;
- Integrating security considerations: all EU legislation, policies and programmes will be prepared, reviewed and implemented with a security perspective in mind;
- Doing serious investments: the EU, the Member States and the private sector must ensure that sufficient human and financial resources exist, public spending for security is increased and security research is promoted, so that the EU’s strategic autonomy is enhanced.

The Commission also outlines a new European internal security governance, which will include:

- Consistently identifying potential security and preparedness implications of new and revised Commission initiatives from the start and throughout the negotiation process;
- Regular meetings of the Commission Project Group on European Internal Security, supported by strategic cross-sectoral collaboration across the Commission;
- Presentations of the threat analyses related to internal security to support the work of the Security College;
- Discussions with Member States in the Council on the evolving internal security challenges based on the threat analysis and exchange on key policy priorities;
- Regular reporting to the European Parliament and the Council to track and support systematic implementation of key security initiatives.

The Strategy lists several subject matters in which the Commission sees the need for action in the future, such as stronger JHA agencies, critical communication, lawful access to data, strengthened border security, critical infrastructure and cybersecurity. Measures will be guided by the following basic objectives:

- Equipping the EU with new ways of sharing and combining information and providing a regular EU internal security threat analysis, which contributes to a comprehensive risks and threats assessment;
- Developing new tools for law enforcement, such as a revamped Europol, and better means of coordinating and ensuring secure data exchange and lawful access to data;
- Building resilience against hybrid threats by enhancing the protection of critical infrastructure, reinforcing cybersecurity, securing transport hubs and ports and combatting online threats;
- Fighting organised crime by proposing stronger rules to tackle organised crime networks, including on investigations, making youth in the EU less vulnerable to recruitment into crime, and stepping up measures to cut off access to criminal tools and assets;
- Introducing a comprehensive counter-terrorism agenda to prevent radicalisation, secure online and public spaces, throttle financing channels and respond to attacks when they occur;
- Making the EU a stronger global player on security, e.g. by boosting operational cooperation with key regions such as neighbourhood countries and Latin America.

*Background:* The Commission's Communication on the European Internal Security Strategy is one component that sets out a vision for safe, secure and resilient EU, together with the Preparedness Union Strategy, the White Paper on European Defence – Readiness 2030, and the (upcoming) European Democracy Shield. The [Preparedness Strategy](#) presented on 26 March 2025 focused on strengthening civilian and military crisis readiness. The [White Paper on European Defence](#) presented on 18 March 2025 sets out a strategic vision for European defence cooperation, investments, and

industrial capabilities. The [European Democracy Shield](#) will promote and strengthen democratic resilience in the EU. See also the article by E. Saxon, C. Monti and P. Olivares-Martinez, "Security – A Firm Construct or an Undetermined Concept?", in this issue.

*Update:* On 5 May 2025, civil society organisations, scientists, researchers and other experts with expertise in human rights and technology reacted to the Commission new Internal Security Strategy. In a [letter to Henna Virkkunen](#), Executive Vice-President of the Commission for Tech Sovereignty, Security and Democracy, they particularly voiced concerns over the Commission's plans to enable law enforcement authorities access to encrypted data. They stressed that encryption is a vitally important tool for people's rights and freedoms and called on the Commission to allow them a meaningful participation in the discussions to come. (TW)

#### Smart Border Control Technologies: Results of METICOS Project

The EU-funded [METICOS project](#) was initiated in response to an observed lack of acceptance of smart border control technologies, among both travellers and border control agencies. Running from 2020 to 2023, the project aimed to predict and explain the acceptance or rejection of smart border technologies, using this information to help change the trajectory towards the widespread use of no-gate security solutions.

During its run, the METICOS project developed numerous models and solutions for measuring metrics such as technology anxiety and performance expectancy as well as other variables. Behavioural patterns exhibited by people passing through a smart EU border control system, as well as patterns relating to how travellers or border control staff accept smart border control technologies, were identified. Different automated

border control gates were tested using virtual reality, and the level of user acceptance was measured.

On 25 April 2025, the Directorate-General for Migration and Home Affairs [shared information](#) about the project's outcome and its potential to provide border management organisations with evidence-based decision-making tools that balance security with traveller privacy. These tools ultimately enable seamless and secure border crossings, to advance the uptake and acceptance of no-gate border checks and security solutions. (CR)

## Schengen

### 2025 State of Schengen Report

On 23 April 2025, the European Commission presented the [2025 State of Schengen Report](#), reviewing the functioning of the world's largest area of free movement over the past year and outlining the priorities for the year ahead. It is the fourth annual report (for the 2024 report ([→eucrim 1/2024, 8](#)); for the 2023 report ([→eucrim 2/2023, 114–115](#))) and comes ahead of the celebrations on the 40th anniversary of the Schengen Agreement, which was signed on 14 June 1985.

The Commission highlights that the Schengen Agreement has grown into a vital framework for freedom, security, and cooperation across Europe, now encompassing 29 countries with over 450 million residents.

The report emphasises Schengen's evolving role as a strategic asset: supporting the Single Market, strengthening EU-wide security coordination, and fostering unity. In a rapidly changing geopolitical environment, the Schengen area has been described as indispensable for safeguarding both mobility and resilience. The main findings of the 2025 Schengen Report are as follows:



► *Schengen governance strengthened through new tools and cooperation structures*

The 2024–2025 Schengen Cycle introduced several reforms to consolidate political oversight and improve the monitoring of Schengen compliance: The Schengen Barometer+ and Scoreboard were refined to better identify implementation gaps. A Schengen Senior Officials Meeting format was launched to support regular, high-level coordination, focusing on alternatives to internal border controls and reinforcing external border protection. Notably, a common framework for enhanced policy alignment across Member States gained momentum.

► *Schengen expanded with full accession of Romania and Bulgaria*

On 1 January 2025, Romania and Bulgaria fully joined the Schengen area, completing an 18-year process since their EU accession (→[eucrim 4/2024, 266–267](#)). The move is expected to reduce logistics costs for businesses in both countries and eliminate delays caused by internal border checks. The Commission praises this as a milestone for EU integration and a step toward a more cohesive Schengen zone.

Progress toward integration also continued in Cyprus, while Ireland's ongoing evaluation process is expected to be concluded toward the end of 2025, with partial participation in Schengen cooperation already underway.

► *Call for faster digitalisation of borders and visa procedures*

The report identifies digital transformation as a key priority for enhancing Schengen's efficiency and security. Several initiatives are already being implemented or awaiting approval:

- The Entry/Exit System (EES), with a phased roll-out starting October 2025;
- The European Travel Information and Authorisation System (ETIAS), expected in late 2026;

- The EU Digital Travel Document proposal and a unified visa application platform, both planned for 2028.

► *Tightened internal security and return policies*

With threats ranging from organised crime to hybrid warfare, the EU adopted ProtectEU, a new Internal Security Strategy in April 2025 (→[eucrim news of 29 April 2025](#)). The Commission plans to enhance operational police cooperation and improve access to data for security services.

Meanwhile, a thematic evaluation of Member States' return systems has revealed uneven implementation, prompting the Commission to [propose a new legal framework for returns](#) in March 2025. In 2024, nearly 123,400 individuals without legal residence were returned from the EU, a 12% increase from the previous year. Frontex supported over 56,000 of these cases, reflecting growing reliance on joint EU mechanisms.

► *Schengen countries facing pressure to end internal border checks*

Although the Schengen Borders Code was revised in July 2024 to restrict internal border controls, ten Member States – including Germany, France, and Sweden – reintroduced or prolonged such controls (by April 2025). Germany, for instance, extended checks to all internal borders. The Netherlands has also introduced controls at land and air borders for the first time.

The Commission expresses concern that some checks may be disproportionate and highlighted alternatives, such as enhanced police cooperation in border regions. It is conducting structured dialogues to assess these measures and promote better coordination.

► *Persisting operational gaps*

Evaluations conducted in 2024 in countries like Poland, Croatia, and Hungary revealed both improvements and shortcomings in border management. While external border

surveillance has improved, serious deficiencies remained in some Member States – particularly in Hungary and Greece – regarding fundamental rights in return procedures and underuse of IT systems like the Schengen Information System.

Only half of the countries evaluated included photos or fingerprints in security alerts, weakening collective efforts to detect threats. The Commission urges Member States to prioritise investments and align national reforms with available EU funding.

► *Future priorities to focus on governance, security, and digital systems*

Looking ahead, the 2025–2026 Schengen Cycle will prioritise three areas:

- Consolidating governance through stronger political oversight and clearer national coordination;
- Strengthening police cooperation to address transnational threats using a “whole-of-route” approach;
- Accelerating digitalisation of border management and visa systems to ensure timely and effective rollout.

The Commission called on the Schengen Council to endorse these priorities at its next meeting in June 2025. (AP) ■

**Bavarian Court: 2022 Border Check near German-Austrian Border Unlawful**

The Bavarian Administrative Court (*Bayerischer Verwaltungsgerichtshof [BayVGH]*, Germany) ruled on 17 March 2025 ([Case No. 10 BV 24.700](#)) that a border check carried out on a train near the German-Austrian border in June 2022 was not compliant with the Schengen Borders Code and thus unlawful.

The claimant, international law scholar *Stefan Salomon*, junior professor of European law at the University of Amsterdam, had previously brought a similar case concerning border checks in Austria before the Court of Justice

of the European Union (CJEU) ([Case C-368/20, NW v Landespolizeidirektion Steiermark](#)). In this case, which concerned checks by Austria at its border to Slovenia, the CJEU ruled on 26 April 2022 that the Schengen Borders Code precludes border control at internal borders from being temporarily reintroduced by a Member State on the basis of a serious threat to its public policy or internal security if the duration of its reintroduction exceeds the maximum total duration of six months and no new threat exists that would justify applying afresh the periods provided for by the code ([→eucrim 2/2022, 89](#)).

Following this line of argument, the BayVGH held that the identity check, conducted by the German Federal Police on an ICE train near Passau, violated the Schengen Borders Code because the prolongation of the reintroduction of border controls in spring 2022 by German Minister of Interior, *Nancy Faeser*, lacked a sufficiently new factual basis, and a mere reassessment of an unchanged situation did not justify the measure.

While the lower administrative court in Munich had initially dismissed the claim as inadmissible, the higher administrative court (BayVGH) acknowledged a risk of recurrence and allowed the appeal. The judgment underscores the requirement that any reintroduction of internal border controls within the Schengen Area must be based on new circumstances.

Since taking office in early May 2025, the new German government under Chancellor *Friedrich Merz* has tightened border controls along the German borders, including to Austria, in order to target illegal asylum seekers. In its [press release](#), the BayVGH stressed that it only had to rule on the specific identity check carried out on the claimant on 11 June 2022 as part of the border controls carried out at that time, not on the general admissibility of internal border controls. Nonetheless, the ruling may contribute to

the controversial discussion on whether the tightened border controls of the new German government are in line with EU law. (AP)

## Ukraine conflict

### CJEU Rulings on EU's Restrictive Measures against Russia (January – April 2025)

This news item summarises rulings by the Court of Justice of the European Union (CJEU), i.e. General Court (GC) and Court of Justice (ECJ), taken in the period between January 2025 and April 2025 in relation to EU sanctions against Russia in response to its war in Ukraine (see also the overview at [eucrim 2/2024, 89–91](#)).

■ **22 January 2025:** The GC [confirms the EU's decision](#) to put *Andrey Melnichenko*, a Russian industrialist, under sanctions targeting those undermining Ukraine's sovereignty. Melnichenko, former owner of major Russian fertiliser and coal companies (EuroChem and SUEK), challenged his listing, but the Court rejects his arguments ([Case T-271/22](#)). The EU based the listing on Melnichenko's status as a leading businessman in sectors that provide significant revenue to the Russian government (fertilizers and energy). His presence at a February 2022 meeting with Putin, shortly after the invasion began, further supported this designation. Despite Melnichenko's claim of having transferred his assets to a trust and later to his wife, the GC finds that he retains economic benefits and influence. It also rules that the sanctions are proportionate and serve the EU's goal of increasing pressure on Russia. Lastly, the GC emphasised that the EU does not need to prove a personal link to the Russian government if the individual plays a leading role in key economic sectors.

■ **29 January 2025:** In [case T-1106/23, Vinokurov v. Council](#), the GC dismisses the action brought by Russian busi-

nessman *Alexander Vinokurov*, confirming the legality of his inclusion on the EU sanctions list. Vinokurov had contested several Council acts from 2023 and 2024 that maintained his listing in connection with Russia's war against Ukraine. The Council justified his listing on the basis of a new criterion introduced in 2022, which targets individuals operating in sectors that constitute a substantial source of revenue for the Russian government. The Council relied on Vinokurov's involvement in key Russian companies as well as his personal connections – most notably his marriage to the daughter of Foreign Minister *Sergey Lavrov* – and his presence at a meeting with President Putin on 24 February 2022. [The GC finds](#) that the new criterion used by the Council was sufficiently precise: it does not require the individual to actively support the Russian government, but merely to be engaged in economic activities that generate substantial revenue supporting it. It holds that the Council had not committed any manifest error of assessment in concluding that Vinokurov's business activities fell within this scope. The restrictive measures were proportionate in light of the EU's objective of increasing pressure on Russia to end its military aggression against Ukraine. With respect to legal certainty, the Court emphasises that the Council is required to conduct periodic reviews of listings and that individuals may submit requests for delisting at any time.

■ **13 March 2025:** The ECJ dismisses an appeal brought by former Russian Deputy Prime Minister, *Igor Shuvalov* ([Case C-271/24 P](#)). Shuvalov appealed a judgment of the GC that confirmed his inclusion on the list of persons covered by EU restrictive measures due to Russia's war against Ukraine. [The ECJ observes](#), in particular, that the GC did not err in law in holding that the Council could rely on positions held and public statements made by Mr Shuvalov prior to the adoption of the



acts at issue. The GC also correctly held that the Council had established that Mr Shuvalov supported actions or policies targeting Ukraine. There were sufficient reasons for the listings in question. Lastly, the ECJ confirmed the GC's position that the acts in question do not undermine the essence of Mr Shuvalov's right to property and that the limitation imposed by the restrictive measures on that right does not appear to be manifestly inappropriate in relation to the objective which they pursue.

■ **19 March 2025:** The [GC dismisses an action brought by a Belarusian iron and steel company](#) that was included in the EU sanctions list in view of the serious situation in Belarus and Belarus' participation in Russia's aggression against Ukraine ([Case T-1042/23, "BMC" holding v Council](#)). The GC first rejects the company's arguments that the Council made an error of assessment because the company is not an important source of income for the Lukashenko regime, does not benefit from that regime or support it, and is not responsible for repression against civil society in Belarus. The GC points out, *inter alia*, that the applicant is recognised by President *Lukashenko* as one of the "flagships" of Belarus, is one of the five largest companies in the country, exports its products to more than 60 countries worldwide and has paid dividends amounting to millions of euro to the Belarusian State. Furthermore, the applicant has not provided any evidence to the contrary that it has not 'benefited' from the Lukashenko regime. This is supported by evidence, correctly accepted by the Council, that the applicant has benefited from extensive state subsidies and political support from the Lukashenko regime and that its general director was personally appointed by President Lukashenko. Finally, the Court rejects the argument that the freezing of funds imposed on the company constitutes a restriction on the exercise

of the rights and freedoms recognised in the Charter and their essence. The conditions of Art. 52(1) of the Charter are met, and no disproportionate interference with the applicant's right to property and freedom to conduct a business can be found in the EU sanctions regime.

■ **26 March 2025:** An action by Dutch media outlets against restrictive measures taken by the Council in view of Russia's actions destabilising the situation in Ukraine turns out unsuccessful before the GC ([Case T-307/22, A2B Connect BV and Others](#)). The applicants (who are established in the Netherlands and are providers of internet services to individuals and to businesses) proceed against the Council's ban of broadcasting and advertising products in Russia following its military aggression against Ukraine. [The GC first ruled](#) that it has no jurisdiction as regards the Council Decisions adopted in the context of the common foreign and security policy (CFSP) because the applicants' names are not on the lists annexed to the contested acts establishing restrictive measures. However, the Court can review the legality of the contested Council Regulations which have been adopted on the basis of Art. 215 TFEU. Second, the GC affirmed that the Council had competence to the regulations concerned. It observes on that point: since the propaganda and disinformation campaigns conducted by media outlets under the control of the leadership of the Russian Federation are capable of undermining the foundations of democratic societies and are an integral part of the arsenal of modern warfare, the restrictive measures at issue are integral to the pursuit by the EU of the objectives assigned to it in Art. 3(1) and (5) TEU. Since the actions in question constitute, in that regard, a significant and direct threat to the public order and security of the EU, those measures, by seeking to

safeguard the values, fundamental interests, security and independence of the EU and to preserve peace, are, therefore, directly linked to the aims of the CFSP. The GC also rejects other pleas brought by the applicants. It rules, *inter alia*, with regard to the freedom to impart information that it was appropriate for the Council to take internet service providers, such as the applicants, into consideration in the same way as any of the means of content transmission or distribution, as operators that are expected to ensure the application and effectiveness of the broadcasting prohibitions in the EU territory.

■ **30 April 2025:** Following a request for a preliminary ruling, the ECJ clarified that EU sanctions against Russia prohibit the export of euro banknotes – even when intended to pay for medical treatments in Russia. ([Case C-246/24, ZZ/Generalstaatsanwaltschaft Frankfurt am Main](#)). The case concerned a traveller stopped at Frankfurt Airport carrying nearly €15,000 in cash. While she claimed the money was to fund medical procedures such as dental treatment, hormone therapy in a fertility clinic, and breast surgery, German customs officers seized most of the amount, allowing only €1,000 for travel expenses. They argued that EU law prohibits the export of banknotes denominated in euro or in any other official currency of a Member State to Russia. This prohibition does not apply only to the sums necessary for the personal use of travellers or those of members of their immediate families travelling with them. The [judges in Luxembourg affirmed](#) that this exception in EU sanctions does not extend to medical expenses. The purpose of the exemption is strictly to cover travel and subsistence, not additional costs like medical treatment. The decision confirms the strict scope of the EU's cash export ban as part of its response to Russia's war in Ukraine. (AP/TW)

## Eurojust Takes Stock of JIT Investigating War Crimes in Ukraine

On 24 February 2025, the day on which Russia started the invasion of Ukraine three years ago, Eurojust [published a summary of the results](#) of the Joint Investigation Team (JIT) on alleged core international crimes (CICs) in Ukraine. The JIT was set up in March 2022 ([→eucrim 2/2022, 79–80](#)) and comprises the following countries: Estonia, Latvia, Lithuania, Poland, Romania, the Slovak Republic and Ukraine ([→eucrim 1/2024, pp 8–9](#)). Since the JIT's establishment, it has been supported by Eurojust, the United States Department of Justice (DOJ), the International Criminal Court (ICC), Europol, the Core International Crimes Evidence Database ([CICED](#)), and the International Centre for the Prosecution of the Crime of Aggression against Ukraine ([ICPA](#)).

The results of their combined actions include:

- 4000 witnesses interviewed so far by the national authorities participating in the JIT;
- Over 40,000 interviews conducted by the Ukrainian authorities on their own territory;
- Notices of Suspicion *in absentia* against six suspects issued by the Lithuanian Prosecution Service;
- One Notice of Suspicion for war crimes against a civilian issued by the Office of the Prosecutor General of Ukraine;
- 26 coordination meetings between the JIT and other national authorities investigating alleged core international crimes (CICs) committed in Ukraine organised by Eurojust;
- Compilation of a case-building package by the ICPA, intended for transmission to the future office of the prosecutor of a possible special tribunal or other jurisdictions;
- Collection and analysis of potential evidence by the ICPA;
- Submission of more than 3700 evidence files by 16 countries to the CICED;

■ Introduction of new translation tool to translate evidence files submitted by national authorities (for translation from 19 languages into English).

Since the beginning of the war, Eurojust has been at the forefront of supporting accountability for Russian crimes. Eurojust has provided legal and analytical expertise as well as logistical and financial support to the JIT. The Agency has also allocated roughly half a million euros to finance the JIT's activities. (CR)

## ECA: Crisis-Related Measures Must be Accompanied by Appropriate Monitoring System

On 12 February 2025, the European Court of Auditors (ECA) published its [Special Report 05/2025, titled Cohesion's Action for Refugees in Europe](#), examining how EU cohesion policy funds have supported Member States in managing the 2022 Ukrainian refugee crisis. The report evaluated whether these funds, specifically the CARE (Cohesion's Action for Refugees in Europe) initiative and the REACT-EU programme, provided timely and effective support and whether the resources were used efficiently and appropriately.

Following Russia's invasion of Ukraine, over four million displaced persons, mostly women and children, were granted temporary protection across the EU. In response, the European Commission introduced the CARE initiative in March 2022, allowing Member States to reallocate cohesion policy funds and simplify procedures to support refugees. This followed the broader REACT-EU initiative launched during the COVID-19 crisis.

The ECA found that the flexibility granted by CARE helped Member States respond quickly to the refugee influx. However, due to the retrospective nature of the funding and the delayed implementation of some projects, the immediate needs of refugees were often met with pre-existing

national resources. The auditors noted that Member States mainly used EU funding for short-term support, such as accommodation, food, and health-care, but invested less in longer-term integration measures like language training or employment assistance.

The report revealed that, although cohesion policy funding provided useful support, the Commission could not fully assess the extent of CARE's actual contribution. The lack of targeted reporting requirements made it difficult to measure/monitor the results and effectiveness of this financial assistance.

The ECA recommended the following:

- The Commission should improve its ability to track and assess how cohesion funds are used to support displaced persons by establishing clearer reporting and evaluation mechanisms;
- In the event of future crises, better preparedness should include mechanisms to track funding allocations and outcomes more precisely;
- Member States should be encouraged to use EU funds not only for emergency needs but also for longer-term integration measures to ensure sustainable support for refugees. (AP)

## EU Reactions to Russian War against Ukraine: Overview End of January 2025 – April 2025

This news item continues the reporting on key EU/CoE reactions following the Russian invasion of Ukraine on 24 February 2022: the impact on the EU's internal security policy, on criminal law, and on the protection of the EU's financial interests.

The following overview covers the period from the end of January 2025 to the end of April 2025. For overviews of developments in previous periods [→eucrim 4/2024, 267–268](#) and [→eucrim 3/2024, 174–176](#), each with further references.

- 27 January 2025: The Council of the EU [adds three Russian military](#)

[officers to its cyber sanctions list](#) for their role in malicious cyberattacks against Estonia in 2020. All three are part of GRU Unit 29155, a covert Russian military unit known for operations across Europe. The cyberattacks breached Estonian government ministries, stealing thousands of confidential documents, including business secrets and health records. Unit 29155 has also carried out cyberattacks on other EU Member States and Ukraine. Individuals and entities appearing on the EU cyber sanctions list are subject to an asset freeze and a travel ban; EU persons and entities are prohibited from making funds available to those listed.

■ **4 February 2025:** Europe takes a major step toward establishing a Special Tribunal to prosecute the crime of aggression committed by Russia against Ukraine. Senior legal experts of the European Commission, the European External Action Service, the Council of Europe, Ukraine and 37 States [lay out the legal foundations for the establishment of this Special Tribunal and introduce the “Schuman Draft Statute”](#), which will govern the tribunal. Once established, the tribunal will hold Russian political and military leaders accountable for initiating the war. Commission President *Ursula von der Leyen* declares this as justice in motion, adding that Russia must not only face trial but also compensate victims. The EU also supports the creation of an International Claims Commission for Ukraine, tasked with assessing and awarding compensation for damages recorded in the Register of Damage. Negotiations for the Claims Commission were set to begin by end of March 2025, while the Council of Europe will coordinate the final legal steps for the tribunal’s creation.

■ **24 February 2025:** The Council adopts the [16th sanctions package](#) in response to Russia’s war of aggression against Ukraine. The package adds 48 individuals and 35 entities to

the EU’s list of targeted restrictive measures. The listing includes Russian military-industrial companies, oil transport entities, sanctions evaders, a Russian crypto exchange (Garantex), and foreign actors, who directly support the Russian war. In addition, the 16th sanctions package takes measures against vessels (“Russian’s shadow fleet”) and companies which are engaged in sanctions circumvention. A series of measures also further curb trade with Russia. These measures include an extension of the ban on imports of Russian aluminum, an extension of dual-use export restrictions, and an extension of the prohibition to provide goods, technology and services for Russia’s energy industry. Moreover, the EU takes action to prevent financial flows from being diverted via smaller banks. In this context, 13 financial institutions are added to the list of entities subject to the prohibition to provide specialised financial messaging services; 3 banks are added to the transaction ban due to their use of the Financial Messaging System of the Central Bank of Russia (SPFS) to circumvent EU sanctions. The EU can now also provide a transaction ban to financial institutions and crypto asset providers that participate in the circumvention of the Oil Price Cap and facilitate transactions with listed vessels of the shadow fleet. Finally, the sanctions package suspends broadcasting activities of additional eight media outlets in the EU or directed at the EU for their dissemination of disinformation on Russia’s war in Ukraine.

■ **24 February 2025:** Remembering the third anniversary of the start of Russia’s full-scale aggression against Ukraine, the Council of Europe Secretary General *Alain Berset* publishes a [report summarising the key responses of the Council of Europe](#) to help Ukraine since the first day of the war. Council of Europe’s actions include the exclusion of the Russian Federation

from the Council of Europe in March 2022, the adoption and implementation of the Action Plan for 2023–2026 to support Ukraine’s resilience, recovery and reconstruction, work to hold Russia accountable for its illegal war of aggression, and helping children of Ukraine. The report also mentions the [Register of Damage Caused by the Aggression of the Russian Federation against Ukraine](#), which was first mooted by the CoE Parliamentary Assembly in October 2022, and subsequently set up in May 2023, as well as the ongoing work on establishing a Special Tribunal for the Crime of aggression against Ukraine within the Council of Europe (see above). In the foreword of the report, *Alain Berset* wrote: “The fight for Ukraine is a fight for justice, recovery and the right of the Ukrainian people to shape their own destiny.”

■ **27 February 2025:** On occasion of the third anniversary of Russia’s full-scale invasion of Ukraine, the Presidents of the European Parliament, European Council, and European Commission [reaffirm the EU’s steadfast support](#) for Ukraine’s sovereignty, resilience, and path toward EU membership. They emphasise that Russia bears full responsibility for the war and its crimes, and support ongoing efforts to establish a Special Tribunal to hold those accountable (see also above).

■ **6 March 2025:** The heads of state or government of the EU Member States convene for a [special European Council meeting](#) to discuss Ukraine and European defence. [They 26 leaders reaffirm](#) the EU’s unwavering support for Ukraine’s independence, sovereignty, and territorial integrity in the face of Russia’s ongoing war (Hungary did not consent to the conclusions). The EU commits to strengthening Ukraine’s defense and military capabilities, pledging €30.6 billion in support for 2025 – €12.5 billion through the Ukraine Facility and €18.1 billion from the G7 ERA initiative, financed through profits from immobilized Russian assets.

The European Council called on the Commission to swiftly take all necessary measures to frontload financing under these instruments and urged the Commission and Member States to use all options under the Ukraine Facility to increase support to Ukraine. Furthermore, the leaders set principles for “a comprehensive, just and lasting peace based on the principles of the UN Charter and international law”.

■ **7 March 2025:** At the Justice and Home Affairs Council, EU justice ministers [discuss accountability for crimes linked to Russia’s war against Ukraine](#). The Polish Council Presidency presents an overview of ongoing initiatives by the EU, its Member States, and international bodies – aimed at ensuring justice. The ministers exchange views on how to best support the future Special Tribunal under the auspices of the Council of Europe (see above), particularly regarding the transfer of evidence stored in the Core International Crimes Evidence Database (CICED) at Eurojust.

■ **12 March 2025:** The [European Parliament adopts a resolution](#) urging the EU and its Member States to significantly increase support for Ukraine, reaffirming the EU’s role as Ukraine’s primary strategic ally and main donor. The resolution supports a European-led enforcement coalition for a future peace agreement and emphasizes that no security talks in Europe should exclude the EU. MEPs criticize the U.S. administration’s shift in tone and urge stronger EU leadership. MEPs also call for the acceleration of Ukraine’s EU accession talks, the confiscation of frozen Russian assets to fund Ukraine’s defense and reconstruction, and tougher sanctions on Russia and any entities aiding in sanctions evasion or supplying military goods.

■ **17 March 2025:** The [Council approves a third payment of nearly €3.5 billion](#) in grants and loans to Ukraine under the Ukraine Facility, bringing total support through the Fa-

cility to almost €20 billion since its launch one year ago. The payment follows Ukraine’s successful implementation of 13 reform steps outlined in its Ukraine Plan. The Ukraine Facility supports Ukraine’s macro-financial stability, recovery, reconstruction, and EU accession process, with a focus on long-term modernisation and reform over the next four years.

■ **20 March 2025:** The [European Council discusses the latest developments](#) with regard to Ukraine. 26 heads of state or government of the EU Member States (Hungary did not consent) reiterate their standpoints voiced in previous meetings. The repeat their firm support for Ukraine’s sovereignty and right to self-defense, committing to ongoing military, humanitarian, and financial aid. The leaders reaffirm their support for a comprehensive peace agreement that must have robust and credible security guarantees for Ukraine to deter future Russian aggression. They stress that the EU is strongly committed to ensure full accountability for war crimes and the other most serious crimes committed in connection with Russia’s war of aggression against Ukraine. In this context, the progress made on establishing a Special Tribunal for the Crime of Aggression against Ukraine, within the framework of the Council of Europe, is seen as an important step.

■ **25 March 2025:** The European Commission [raises €8 billion in its fourth syndicated bond transaction](#) of the year, with part of the funds allocated to support Ukraine. The proceeds contribute to Ukraine’s financing through the Ukraine Facility, which foresees up to €33 billion in loans between 2024 and 2027, and under the exceptional €18 billion Macro-Financial Assistance programme. The Commission has already disbursed nearly €16.2 billion to Ukraine under the Facility and €4 billion through the new ERA loans, which will eventually be repaid using

proceeds from immobilised Russian state assets.

■ **9 April 2025:** The [10th EU-Ukraine Association Council](#) meeting is held in Brussels, discussing progress in EU accession talks, Ukraine’s reform path, and the integration of Ukraine into selected EU policies. It highlights over €144 billion in EU and Member State support to Ukraine, including €49.6 billion in military aid. The Council also acknowledges the G7’s approval of a \$50 billion loan for Ukraine. The meeting addresses accountability for war crimes, welcomes steps toward establishing a Special Tribunal, and reaffirms support for Ukraine’s defence sector, economic recovery, and public administration reform. In the margins of the Association Council, [five new EU-Ukraine agreements are signed](#). They include €300 million in European Investment Bank (EIB) financing for critical infrastructure, Ukraine’s participation in the EU Space Programme, and a joint procurement deal for medical countermeasures, supporting Ukraine’s resilience and recovery.

■ **9 April 2025:** The European Commission [releases another €1 billion to Ukraine](#) through its exceptional Macro-Financial Assistance loan programme. This support, financed by profits from immobilised Russian assets, is part of the G7-led ERA initiative and helps Ukraine meet urgent budget needs, including military and reconstruction efforts. In addition, the EU provides to Ukraine a tranche of €2.1 billion in windfall profits generated from frozen Russian Central Bank assets.

■ **10 April 2025:** The EU and Ukraine agree to extend their [Road Transport Agreement](#) until 31 December 2025. This extension ensures continued facilitation of Ukraine’s access to global markets and strengthens trade flows through smoother transit across EU countries.

■ **14 April 2025:** At the [Foreign Affairs Council meeting](#), [Kaja Kallas](#), High Rep-



representative for Foreign Affairs and Security Policy, stresses that the EU is the greatest supporter of the Ukrainian defence industry, as European countries have so far committed over €23 billion for military aid to Ukraine this year. She announces that the EU is working on a 17th package of sanctions that will focus on the shadow fleet circumventing EU sanctions against Russia and Belarus. (AP/TW)

## Artificial Intelligence (AI)

### European AI Associations Call for European AI Sovereignty

On 29 January 2025, the European AI Forum (EAIF), the AI, Data and Robotics Association (ADRA), and EIT Digital issued a [joint statement](#) addressing recent advances by the United States and China in artificial intelligence initiatives. The statement underscores the need for the European Union to develop a robust, energy-efficient, and strategically autonomous AI infrastructure as a matter of urgency. It is termed the “EU AI Stack” and is intended to foster an open, sovereign, and innovative European AI ecosystem.

The announcement of the STAR-GATE project by U.S. President Trump, involving major partners such as OpenAI, Oracle, and SoftBank, signifies a substantial investment – up to \$500 billion – in expanding AI infrastructure in the United States. Concurrently, China’s commitment, exemplified by the Bank of China’s plan to invest 1 trillion yuan (approximately \$140 billion) in the AI sector over five years, highlights its strategic focus on AI to bolster geopolitical influence.

The joint statement advocates for the European Union to take decisive action by reducing bureaucratic hurdles, stimulating private investment, encouraging entrepreneurial initiatives, and promoting the adoption of European AI solutions across various industries. Failure to act promptly, the

statement warns, could result in Europe lagging behind in global AI development. This would increase dependence on non-European AI providers and compromise the continent’s technological competitiveness and digital sovereignty. (AP)

### Guidelines on Prohibited AI Practices

On 4 February 2025, the European Commission published [non-binding Guidelines on Prohibited Artificial Intelligence \(AI\) Practices](#), pursuant to Art. 5 of Regulation (EU) 2024/1689 (AI Act), which entered into force on 1 August 2024. The AI Act is the EU’s flagship legislation on artificial intelligence, introducing a risk-based framework for AI governance that categorizes AI systems into four levels of risk: unacceptable, high, limited, and minimal. The Guidelines are intended to promote the consistent, effective, and uniform application of the prohibitions set out in the Act and to assist stakeholders in interpreting and operationalizing its provisions.

The Commission clarified that AI practices falling under the unacceptable risk category are those that contravene fundamental rights protected under Union law. These include, *inter alia*, the use of subliminal techniques and manipulative strategies that materially distort user behavior, AI systems exploiting vulnerabilities related to age or disability, social scoring systems based on personal characteristics or behavior, and the use of predictive AI to infer criminal risk solely through profiling. The Guidelines also addressed the prohibition of untargeted scraping of facial images from online sources for biometric identification purposes as well as the use of emotion recognition systems in workplaces or educational settings – except under narrowly defined safety or medical exceptions.

Particular attention was given to real-time remote biometric identification (RBI) in public spaces for law enforcement purposes. While generally pro-

hibited, the Guidelines acknowledged limited exceptions subject to strict legal and procedural safeguards. Further prohibited were biometric categorization systems that infer sensitive attributes such as political orientation or sexual preference, unless demonstrably justified under Union law.

The Guidelines elaborated on both the material and personal scope of the prohibitions. They distinguished between providers and deployers of AI systems and outlined cases in which the AI Act does not apply, such as military applications, national security contexts, and scientific research. Emphasis was placed on ensuring that these exclusions are interpreted narrowly so as not to undermine the protective aims of the AI Act.

In terms of enforcement, the Guidelines reiterated that national market surveillance authorities bear primary responsibility for monitoring compliance. The AI Act empowers these authorities to impose significant administrative fines – up to €35 million or 7% of annual global turnover – for breaches of Art. 5.

The Guidelines concluded that the prohibited AI practices outlined in Art. 5 pose a significant threat to the protection of fundamental rights such as autonomy, privacy, non-discrimination, and human dignity. Accordingly, the Commission recommended a case-by-case approach to interpretation and enforcement, stressing the importance of contextual analysis and the precautionary principle. It is also underscored that institutional coordination is needed, both across Member States and within EU bodies, facilitated by the AI Board, in order to foster coherent implementation. (AP)

### Secretive Security AI Agenda Sparks Concern Over Civil Liberties

The European Union is facing renewed criticism over its secretive development of artificial intelligence (AI) tools for policing, border control, and crim-



inal justice, following a report published by Statewatch in April 2025: [Automating Authority](#). The report reveals that the EU and its Member States have quietly expanded efforts to deploy so-called “security AI” technologies. According to the authors, this development occurred largely outside public scrutiny, despite its far-reaching implications for privacy and civil liberties. They warn of serious threats to human rights, democratic oversight, and accountability.

When the EU adopted the landmark Artificial Intelligence Act in 2024 to regulate high-risk AI systems and uphold fundamental rights, the law included sweeping exemptions for security-related uses. Among the most concerning was a full exemption until at least 2031 for high-risk AI used by public authorities – carve-outs for biometric surveillance, profiling, and data categorisation by law enforcement.

Documents obtained via access to information requests have revealed how internal EU bodies, including the European Clearing Board and eu-LISA, have worked to weaken safeguards and lay the institutional groundwork for security AI deployment. Consultancy firm Deloitte, for instance, had reportedly drafted initial plans for a “centre of excellence” at eu-LISA, although that proposal was later shelved.

The report also sheds light on the technical infrastructure being built to support security AI systems. The Security Data Space for Innovation (SDSI), an EU-funded project, was found to be mapping types of police-held data – including photos, audio data, and scraped web content – for use in AI training. Europol’s parallel initiative included developing an AI “sandbox” to test tools like voice analysis and facial recognition in a controlled environment. Statewatch cautions that these developments risk entrenching bias in policing, especially as AI systems trained using flawed or discriminatory datasets.

[According to Romain Lanneau](#), co-author of the report, EU police and migration authorities would effectively self-assess the legality of their experiments with highly intrusive technologies. This engenders risks such as violations of freedom of expression, the right to asylum, and the principle of non-discrimination. As concerns about AI governance and the influence of far-right actors in Europe grow, the report is calling for robust democratic oversight and urgent public debate on the future of “security AI” in the EU. (AP)

## Digital Space Regulation

### Overview of the Latest Developments on the DSA: February–April 2025

The Digital Services Act (DSA) is designed to foster a safer, fairer, and more transparent online environment ([→eucrim 4/2022, 228–230](#)). It establishes new obligations for online platforms, thereby ensuring that EU users are safeguarded against the dissemination of illicit goods and content and that their rights are respected when they engage in interactions, share information, or make purchases online. The DSA is a crucial touchstone for law enforcement purposes ([→eucrim 1/2024, 13](#)).

This news item continues the reporting on the latest developments concerning the DSA in the form of a chronological overview. It covers the period from February to April 2025. For overviews of the previous developments: April–August 2024 [→eucrim 2/2024, 94–95](#); September–October 2024 [→eucrim 3/2024, 178](#); November 2024 – January 2025 [→eucrim 4/2024, 272–273](#).

■ **6 February 2025:** As part of an ongoing investigation, the European Commission [requests detailed information](#) from the multinational online clothing retailer *Shein*. This includes: internal documents addressing risks related to

illegal goods on its platform, the transparency of its recommender system, and data access for researchers; measures taken to protect consumers, public health, user wellbeing, and personal data. The inquiry is separate from but complements a parallel investigation into *Shein*’s consumer law compliance, led by the Consumer Protection Cooperation (CPC) Network.

■ **19 February 2025:** The Commission [releases a new Research API](#) for the DSA Transparency Database, enabling programmatic access to content moderation data submitted by online platforms across the EU. The database, operational since September 2023, now holds over 26 billion entries, tracking moderation actions with anonymised statements of reasons. The API allows technically skilled users – particularly academic and policy researchers – to query the last six months of indexed data, supporting both longitudinal and cross-platform analysis. Developed in response to feedback from the research community, the tool enhances scrutiny and supports the DSA’s enforcement framework.

■ **20 February 2025:** The Commission [releases a new best-practice toolkit](#) to support application of the DSA during electoral periods. Designed for national regulators – Digital Services Coordinators (DSCs) –, the toolkit offers practical guidance for addressing online risks linked to elections. The toolkit draws from experiences gained over the past year in mitigating threats posed by VLOPs and VLOSEs. It includes strategies to tackle issues such as hate speech, disinformation, online harassment, and manipulation of public opinion, including risks related to AI-generated content and impersonation.

■ **14 March 2025:** Vodafone and other internet providers are taking [legal action against blocking orders](#) issued by the North Rhine-Westphalia State Media Authority (Landesanstalt für Medien Nordrhein-Westfalen [LfM], Germa-

ny) against hardcore sex portals such as Pornhub and YouPorn. Vodafone has filed lawsuits against the orders before the Düsseldorf Administrative Court. In essence, the case centres on whether the LfM still has jurisdiction in this area or whether the Digital Services Act (DSA) now gives sole jurisdiction to the European Commission. The ruling could have far-reaching consequences for the availability of online pornography in Germany.

■ **25 March 2025:** Key signatories of the Code of Conduct on Disinformation – Google, Meta, Microsoft, and TikTok – [publish their latest transparency reports](#), outlining measures taken between July and December 2024 to tackle disinformation. The reports include actions related to the war in Ukraine, the Hamas-Israel conflict, and safeguarding election integrity. This is the fifth such biannual report. Following its endorsement on 13 February 2025, the Code will become a formal part of the DSA framework as of 1 July 2025, serving as a benchmark for DSA compliance under Art. 35.

■ **10 April 2025:** Seven entities found a [European network of out-of-court dispute resolution bodies](#) in accordance with the DSA. The alliance includes dispute resolution bodies from Germany, Ireland, Italy, Malta, Slovakia and Hungary. Out-of-court dispute resolution bodies are one of alternative means foreseen in the DSA to which users can address themselves and request a review of a platform's content moderation decision. Online platforms are obliged to engage with this body. The network aims to exchange information and ideas on mediation work and discuss proven technical standards. The participating entities also hope that the cooperation will simplify interaction with online platforms and regulatory authorities. They also want to better inform the general public about the new user tool.

■ **29 April 2025:** The European Board of Digital Services – an independent

group that advises the Commission on the application and enforcement of the DSA – [holds its 13th meeting](#). The Board, *inter alia*, discussed an upcoming report on prominent systemic risks under Art. 35(2) DSA and the revised draft delegated act on data access. Safeguards for younger users in the digital environment and protection of minors were also discussed. (AP/TW)

#### Overview of the Latest Developments on the DMA: January-April 2025

*Eucrim* has been regularly reporting on the EU's major new legislation regulating the digital space, i.e., the Digital Services Act and the Digital Markets Act ([→eucrim 1/2024, 12–13](#) with further references). The Digital Markets Act (DMA) aims to ensure contestable and fair markets in the digital sector. It regulates gatekeepers, which are large digital platforms that provide an important gateway between business users and consumers, whose position can grant them the power to act as bottlenecks in the digital economy.

The following is an overview of the latest developments that have taken place since the news on the DMA in [→eucrim 4/2024, 178–179](#) (covering the period October-December 2024), and in [→eucrim 2/2024, 95–96](#).

■ **13 January 2025:** The [press reports](#) that the European Commission is asking app developers whether the fee they have to pay to Apple for using alternative app stores (the “core technology fee”) prevents fair competition on Apple's platforms and therefore contravenes the DMA. If so, Apple could face coercive measures and penalties of up to ten percent of its annual turnover.

■ **14 February 2025:** In the dispute with the US over “too excessive” regulation of online services and tech companies by the EU, *Henna Virkkunen*, Executive Vice-President of the European Commission for Technological Sovereignty, Security and Democracy, [promised “simplification and harmoni-](#)

[sation” of EU digital legislation](#) on the sidelines of the Munich Security Conference. As a first step, the aim is to review the Digital Services Act (DSA) and the Digital Markets Act (DMA), as well as the EU AI Act, for possible overlaps.

■ **7 March 2025:** The [High-Level Group for the Digital Markets Act \(DMA\)](#) gathers in Brussels for its fourth meeting, commemorating the first anniversary of the DMA's application and two years since the High-Level Group's creation. Commission's Executive Vice-President *Teresa Ribera* emphasises continued collaboration to ensure the DMA's effective and coherent enforcement. The meeting focuses on recent developments in monitoring and enforcing the DMA, with discussions covering data-related obligations, interoperability, and artificial intelligence. The group also examines ongoing joint efforts between the European Commission and the European Data Protection Board (EDPB), particularly regarding the interplay between the DMA, the General Data Protection Regulation (GDPR), and the DSA.

■ **19 March 2025:** The Commission adopts two binding decisions under the DMA, requiring Apple to enable better interoperability between iPhones, iPads, and third-party devices. The [first set of measures](#) improves access to iOS features for developers of connected devices like smartwatches and headphones. The [second set of measures](#) improves the process for handling developer requests, ensuring more transparency and faster review. These steps aim to foster innovation and consumer choice while ensuring compliance with Apple's gatekeeper obligations under the DMA.

■ **25 March 2025:** The Commission [issues two sets of preliminary findings](#) to American international technology conglomerate Alphabet, accusing it of non-compliance with the DMA. The concerns relate to Alphabet's favouring of its own services in Google Search results and the restrictive

steering practices in its Google Play app store. The Commission finds that Google Search may be giving preferential treatment to Alphabet's own services – such as shopping or hotel bookings – over rivals by displaying them more prominently. In addition, Alphabet allegedly prevents app developers from directing users to alternative purchasing channels, while imposing excessive fees on app developers over extended periods. Alphabet now has the opportunity to respond to and defend its practices. If confirmed, these findings could lead to a formal non-compliance decision under the DMA.

■ 3 April 2025: In the [podcast “Mac & I”](#), Malte Kirchner and Leo Becker explain what has changed and what will change for uses of Apple's iPhone after one year of application of the DMA.

■ 23 April 2025: the Commission [closes its investigation](#) into Apple's compliance with user choice obligations under the DMA, following constructive dialogue and improvements made by Apple. At the same time, the Commission issues preliminary findings indicating that Apple's rules for distributing apps outside the App Store may breach the DMA. Developers face new fees and restrictive eligibility requirements, which the Commission views as disincentivising the use of alternative distribution channels.

■ 23 April 2025: the Commission [fines Apple €500 million and Meta €200 million for violating DMA](#). Apple is found to have restricted app developers from informing users about better offers outside the App Store, breaching its anti-steering obligation. The Commission orders Apple to remove these restrictions and avoid future non-compliant behaviour. Meta is fined for its “Consent or Pay” advertising model on Facebook and Instagram, which failed to offer a proper alternative to users who declined personalised ads. The Commission concludes that Meta did not allow users to refuse data combination freely, as required by the DMA.

Both companies have 60 days to comply. The decisions mark the Commission's first formal findings of non-compliance under the DMA.

■ 24 April 2025: The [US Government reacts sharply](#) to the fines imposed on Apple and Meta (see above). The White House called the fines a “novel form of economic extortion which will not be tolerated by the United States”. It also said that this extraterritorial regulation [DMA] is a barrier to trade and a direct threat to free civil society.

■ 25 April 2025: The Commission publishes its [second annual report on the implementation of the Digital Markets Act \(DMA\)](#), outlining enforcement actions taken throughout 2024. The report details new gatekeeper designations, regulatory dialogues with gatekeepers and third parties, and the initiation of specification and non-compliance proceedings where necessary. It also presents information shared by gatekeepers regarding planned acquisitions and consumer profiling practices. The report highlights the ongoing coordination between the Commission and national authorities to ensure effective and consistent enforcement. Lastly, it summarises the 2024 activities of the High-Level Group on Digital Markets. (AP)

## Institutions

### Commission

#### European Commission Work Programme 2025

On 11 February 2025, the European Commission adopted its [work programme for the year 2025](#). It builds on the commitments in the [Political Guidelines](#) and Commission President Ursula von der Leyen's mission letters. Under the theme “Moving forward together: A Bolder, Simpler, Faster Union”, the programme exhibits a strong focus on simplification. This priority

reflects the need for more opportunities, innovation, and growth for EU citizens and businesses. Administrative burdens are to be reduced by at least 25%, and by at least 35% for small- and medium-sized enterprises (SMEs). The key areas of the work programme are:

- A new plan for Europe's sustainable prosperity and competitiveness;
- A new era for European Defence and Security;
- Supporting people, strengthening societies and the European social model;
- Sustaining the quality of life in Europe: food security, water, and nature;
- Protecting democracy, upholding the EU's values;
- Global Europe: Leveraging power and partnerships;
- Delivering together and preparing the Union for the future.

[Omnibus packages](#) and proposals will simplify EU policies and legislation in all these areas, making them work better and faster. The first series of omnibus packages will be on sustainability and investment simplification. A further omnibus package is to follow, addressing small and medium-sized enterprises and the removal of paperwork requirements, a digital package, and a simplification package for the Common Agricultural Policy. Other examples of key initiatives with a significant simplification dimension include the Industrial Decarbonisation Accelerator Act and review of the Securitisation Framework.

In the area of security, the Commission highlights the Preparedness Union Strategy, which will deal with the enhancement of Europe's capability to prevent and respond to emerging threats. In addition, a comprehensive set of actions enabling the anticipation of threats and strengthening the EU's resilience and capabilities to prevent and respond to new and existing crimes and threats will be outlined in the new Internal Security Strategy. The Firearms Trafficking Directive will

provide common criminal law standards on illicit firearms trafficking. Initiatives are planned for the prevention of cybersecurity incidents and a better protection of Europe's undersea infrastructure, notably telecommunications cables, which have increasingly been subject to hybrid threats. The regulation on combating the sexual abuse of children and the anti-smuggling directive are to be finalised.

In total, the 2025 work programme includes 51 new policy initiatives, 37 evaluations and fitness checks, and 123 finalised proposals from previous years. However, 37 proposals will not be pursued, and four Regulations will be repealed. Among the legislative initiatives to be withdrawn are the proposals for a new Regulation on Privacy and Electronic Communications and for a Directive on adapting non-contractual civil liability rules to artificial intelligence. (CR)

## Europol

### Europol and Egypt Sign Working Arrangement

On 9 April 2025, [Europol and the Arab Republic of Egypt signed a Working Arrangement](#) to enhance their cooperation in preventing and combating serious crime, including migrant smuggling, trafficking in human beings, drug trafficking, and child sexual exploitation. The arrangement provides for a structured and enhanced exchange of information on transnational, serious, and organised crime as well as the deployment of a liaison officer at Europol's headquarters in The Hague. It does not, however, provide a legal basis for the transfer of personal data. This is the first such arrangement between Europol and an African country. (CR)

### Cooperation Agreement between Europol and Brazil

On 6 March 2025, the EU and Brazil signed an international [agreement](#) to

strengthen the partnership between Europol and Brazilian law enforcement authorities in the fight against serious and organised crime. Under the agreement, the parties will be able to exchange operational information.

Brazil is the first country in Latin America to sign such an agreement with the EU. The agreement must now be approved by the European Parliament before it can be implemented. Europol pointed out that Brazil has been a strong partner for operational law enforcement cooperation across various crime areas in recent years. Successful law enforcement actions with Brazil include the fight against drug trafficking, cybercrime and human trafficking. (CR)

### Europol Enhances Law Enforcement Cooperation with the Gulf States

With the objective of enhancing cooperation between the Gulf Cooperation Council Police (GCCPOL) and Europol in the fight against organised crime and terrorism, the [first meeting](#) of senior law enforcement officials took place in Abu Dhabi on 5 and 6 February 2025. GCCPOL is a regional law enforcement organisation established by the member states of the Gulf Cooperation Council (GCC): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. It acts as a hub for police cooperation and criminal intelligence sharing between these countries.

The first meeting was attended by law enforcement officials from the above-mentioned countries, law enforcement officials from EU Member States, and representatives from GCCPOL and Europol. Both organisations reaffirmed their commitment to enhance cooperation on the basis of a Letter of Intent signed in 2017. The following common security threats are to be tackled in the future:

- Cybercrime;
- Financial crime;
- Money laundering;

- Online child exploitation;
- Human trafficking;
- Environmental crime. (CR)

### Europol Tackles Violence-as-a-Service

In response to the growing trend of Violence-as-a-Service (VaaS) and the recruitment of young people into serious organised crime, Europol launched a new [Operational Taskforce named GRIMM](#) at the end of April 2025. VaaS often involves young perpetrators who carry out threats, assaults, or killings for a fee, thereby reducing the risk to criminal networks and shielding them from law enforcement. These acts are often orchestrated remotely, with young people recruited and instructed online.

Led by Sweden, the new taskforce brings together law enforcement authorities from Belgium, Denmark, Finland, France, Germany, the Netherlands, and Norway, with Europol providing operational support, threat analysis, and coordination. The taskforce aims to coordinate intelligence sharing and joint investigations across borders, map the roles, recruitment methods, and monetisation strategies used by VaaS networks, and identify and dismantle the criminal service providers that enable such violence. Cooperation with tech companies is also a priority to detect and prevent recruitment on social media.

In addition, Europol has published a [notification](#) that breaks down the recruitment ecosystem, detailing the use of encrypted messaging apps, social media, lifestyle messaging, manipulation tactics, and gamification. The notification explains how criminal networks exploit minors, particularly through recruitment and task assignments via social media. It highlights the use of targeted language, coded messaging, and gamification strategies in this process.

Lastly, Europol has created [an awareness guide](#) for parents, which contains a list of warning signs. (CR)



### SIENA Reaches 3500 Connections

On 3 February 2025, [Europol informed](#) the public that it has expanded its Secure Information Exchange Network Application (SIENA) from 3,000 to 3,500 connections. SIENA enables the secure, efficient, and timely exchange of information between Europol and its partners, including national, regional, and local law enforcement authorities as well as customs officials, border guards, and other specialised police forces.

Under the [Directive 2023/977](#) on the exchange of information between the law enforcement authorities of the EU Member States, which took effect at the beginning of the year, SIENA has also become the “default channel” for cooperation between European law enforcement authorities: SIENA is used by the authorities to send requests for information, to provide information pursuant to such requests, and to provide information on their own initiative. (CR)

### Eurojust

#### Eurojust and the Republic of Korea Sign Working Arrangement

On 30 April 2025, [Eurojust and the Republic of Korea signed a Working Arrangement](#) to enhance their cooperation in the fight against serious and organised crime. The arrangement facilitates strategic collaboration and the exchange of information between Eurojust and the authorities of the Republic of Korea (South Korea) as well as the establishment of Eurojust contact points. It does not permit the exchange of operational personal data. The Republic of Korea is the first Asian country to sign such an arrangement with Eurojust. (CR)

#### Eurojust and Egypt Sign Working Arrangement

On 10 April 2025, Eurojust and the Public Prosecution Office of the Arab Republic of [Egypt signed a Working](#)

[Arrangement](#) to enhance their cooperation in the fight against serious organised crime. This is an EU-funded project implemented by Eurojust to strengthen strategic and operational cooperation in criminal judicial matters with the EU and partners in the Southern Neighbourhood.

The arrangement amends existing cooperation, such as support for Egyptian contact points for Eurojust and cooperation under the EuroMed Justice project. It does not permit the exchange of personal data. (CR)

#### Eurojust Launched New War Crimes & Genocide Project: National Authorities Against Impunity

The increase in armed conflicts worldwide has also led to a significant increase in the number of core international crimes (CICs). In response to this increase, Eurojust and the Genocide Network Secretariat at Eurojust [launched a new project](#) to combat impunity for war crimes, genocide, and crimes against humanity on 12 February 2025. The new project, entitled “[National Authorities Against Impunity \(IMPNA\)](#)”, aims to reduce safe havens for the perpetrators of CICs and thereby contribute to criminal accountability for such crimes. Over the next four years, the project will support civil society organisations (CSOs) in their efforts to document CICs and serious human rights violations; it will pursue avenues of accountability at regional and local levels and establish platforms for cooperation with national judicial authorities to investigate and prosecute CICs in both EU and non-EU countries. The project will also support the efforts of national authorities of non-EU countries in investigating and prosecuting CICs, including by strengthening regional cooperation. In order to achieve this objective, the following measures will be taken:

- Facilitation and application of cooperation and information exchange between CSOs and national authorities

that are investigating and prosecuting;

- Creation of specialised units and development of technical expertise on CICs among national investigating and prosecuting authorities in non-EU countries;

- Creation of regional networks focusing on the investigation and prosecution of CICs in order to enable close cooperation and coordination between the national authorities of non-EU countries in various regions of the world, modelled on the EU Genocide Network;

- Application of a transparent methodology in line with international standards. Project activities will be designed and delivered in line with international human rights standards that integrate a gender-sensitive perspective at all stages of the project implementation. The implementation of project activities will also integrate a victim- and survivor-centred approach and a “do no harm” approach.

- Close coordination with key stakeholders in the global fight against impunity, such as the civil society-led consortium Global Initiative Against Impunity (GIAI), the International Criminal Court (ICC), the Office of the United Nations High Commissioner for Human Rights (OHCHR), UN investigative mechanisms, and other regional partners to identify synergies and avoid duplication of efforts.

The project is funded by the European Commission’s Directorate-General for International Partnerships (DG INTPA) and runs until September 2028. (CR)

#### JIT Against Foreign Terrorist Fighters Leads to Convictions

On 15 April 2025, Eurojust [presented an interim evaluation](#) of a Joint Investigation Team (JIT) into crimes against Ezidi victims in Syria and Iraq.

In 2021, the judicial authorities of Sweden and France set up the JIT, supported by Eurojust, which Belgium and other countries later joined. The JIT had been set up to identify foreign



terrorist fighters (FTFs) with links to the [jihadist group ISIL](#) (Islamic State of Iraq and Syria, also known as Da'esh), who had returned from Syria or Iraq and were involved in core international crimes, primarily against Ezidi victims.

As a result of the JIT's work, in 2024, a Dutch citizen was identified and sentenced to ten years' imprisonment for crimes against humanity. A Swedish citizen was sentenced in 2025 to 12 years' imprisonment for genocide, crimes against humanity, and war crimes committed against nine Ezidi victims. In 2026, a French citizen might be tried on charges of genocide and crimes against humanity.

Although the United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ Islamic State in Iraq and the Levant (UNITAD), which provided important information to the JIT, was closed down in September 2024, the work of the JIT will continue. Based on the principle of universal jurisdiction, EU Member States can investigate core international crimes committed outside their own territory. (CR)

#### New Representative for Denmark at Eurojust

At the beginning of March 2025, Ms [Kirstine Trolborg](#) took up her duties at Eurojust as the new Representative of Denmark. She was previously Head of International Affairs at the Danish Office of the Director of Public Prosecutions. She succeeds Mr *Torben Thygesen*.

Following implementation of the Eurojust Regulation and the [Agreement](#) on cooperation in criminal matters between Eurojust and the Kingdom of Denmark, Denmark has a Representative at the Agency instead of a National Member. Representatives do not have the same level of integration as National Members into Eurojust's organisational structure; they primarily serve as a link between their home country and Eurojust.

Prior to her appointment as Representative of Denmark at Eurojust, Ms Trolborg served as Head of International Affairs at the Office of the Director of Public Prosecutions and she has been involved in various criminal cases requiring international collaboration. Furthermore, she represented Denmark in international negotiations on legal instruments and participated in cross-border judicial networks. (CR)

#### New National Member for the Czech Republic at Eurojust

On 5 March 2025, [Pavel Zeman](#) re-joined Eurojust as National Member for the Czech Republic. Following his service as the first Czech National Member of Eurojust in 2004, Pavel Zeman had returned to the Czech Republic in 2011 and served as its Prosecutor General. Mr Zeman has been appointed for a period of five years. He succeeds *Lukáš Stary*.

Mr Zeman has long-standing experience as public prosecutor in the Czech Republic and has been specialised in cross-border judicial cooperation in criminal matters. After his term as Prosecutor General of the Czech Republic (2011–2021) he became a specialised prosecutor in cybercrime, the criminal liability of legal entities and war crimes and he led the Internal Audit Department of the Czech National Bank prior to his appointment to Eurojust. (CR)

#### New National Member for Slovakia at Eurojust

At the end of 20 January 2025, Mr [Branislav Boháčik](#) started his five-year term as National Member for Slovakia at Eurojust, succeeding Mr Ladislav Hamran, former National Member for Slovakia and President of Eurojust. Prior to joining Eurojust, Mr Boháčik worked as a judicial cybercrime specialist in the international department of the Slovak Prosecutor General's Office. In this capacity, he also gained extensive experience in working with

Eurojust as a Member of the Board of the European Judicial Cybercrime Network (EJCN). He was also head of the Slovak delegation to the Conference of the Parties of the Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds of crime and the financing of terrorism and was the Chair of the Conference between 2015 and 2019. (CR)

#### Frontex

##### Frontex and the European Commission Sign Working Arrangement on Migration Management

On 25 February 2025, Frontex and the European Commission signed [a working arrangement](#) to enhance their cooperation in the field of migration management. Under the arrangement, the parties agree to strengthen situational awareness, early warning, and forecasting. The arrangement is part of Frontex's participation in the Migration Preparedness and Crisis Blueprint Network, a soft law instrument to support the EU's emergency and crisis response functioning in two stages:

- The first stage on monitoring and preparedness aims at a more coordinated use of existing legislation by reinforcing and sharing common situational awareness between all actors involved, developing an early warning/forecasting system at the EU level, and supporting the development of the necessary resilience in EU Member States in order to deal efficiently with any type of migration crisis;
- The objective of the second phase is to support a rapid, efficient, and coordinated EU response to a migration crisis by providing EU decision makers with timely and up-to-date information on the evolving operational situation and by supporting monitoring, coordination on the ground, and communication at the technical level between all actors. (CR)

### AI in Search and Rescue Operations

On 25 and 26 February 2025, Frontex hosted an international [workshop on AI and unmanned systems](#) together with the Italian Coast Guard, which is chairing the European Coast Guard Functions Forum (ECGFF). The workshop, entitled “Coast Guard Evolution: Artificial Intelligence and Unmanned Systems Enhancing SAR Operations”, aimed to explore ways to foster close and effective cooperation between coastguard functions in order to enhance Europe’s collective ability to secure its waters and protect lives at sea. It explored the legal, operational, and technological implications of the introduction of AI in Search and Rescue (SAR) operations. More than 100 participants from 22 Member States, the EU Commission, the European Defence Agency (EDA), the Joint Research Centre (JRC), the European Fisheries Control Agency (EFCA), and the European Maritime Safety Agency (EMSA), together with leading experts in AI and emerging technologies, discussed and shared knowledge on the following topics:

- Benefits and limitations of emerging technologies in both manned and unmanned SAR missions;
- EU initiatives supporting the development of AI-driven tools for coast guard functions;
- The role of networks such as the European Border Surveillance System (EUROSUR) in optimising the cross-border coordination of SAR efforts in migrant emergencies at sea.

Above all, participants agreed that the human element must remain at the heart of any consideration of AI in SAR. Technology must serve humanity. (CR)

### European Data Protection Supervisor (EDPS)

#### EDPS 2020–2024 Mandate Review

The year 2024 marked the conclusion of the EDPS Strategy 2020–2024,

which aimed to shape a safer, fairer, and more sustainable digital Europe ([→eucrim 1/2020, 102](#)). To this end, on 6 March 2025, the EDPS published [a review of its activities](#) during this period.

While the mandate began under the unexpected circumstances of the COVID-19 pandemic, much of the focus subsequently shifted to anticipating future privacy challenges. This involved gaining a better understanding of forthcoming developments in the technology sector from a privacy and data protection perspective. One example of this is the TechSonar project ([→eucrim 4/2022, 238–239](#)), launched in 2021. In addition, the TechDispatch project, which provides a closer and more in-depth look at specific technologies that may have a significant impact on privacy and data protection, received the Global Privacy and Data Protection Award 2021 in the Education and Public Awareness category.

Over the course of this mandate, the EDPS issued Opinions, Joint Opinions with the European Data Protection Board (EDPB), and Formal Comments, and also responded to informal consultations on a range of topics. In the area of Justice and Home Affairs, the EDPS published Opinions on legislative proposals such as the expansion of Europol’s mandate, the EU Police Cooperation Code package, and regulations on the collection and transfer of Advance Passenger Information (API), as well as on a number of international agreements on the exchange of personal data between Europol and Eurojust and the competent authorities of non-EU/EEA countries, and others. Additionally, the EDPS issued a series of Formal and Informal Comments on draft implementing and delegated acts related to the development and use of EU large-scale IT systems (LSITS), including Eurodac, the Schengen Information System (SIS), and the Visa Information System (VIS). The EDPS also contributed to the debate

on highly intrusive modern spyware and closely monitored the challenging and complex discussions on the retention and access to electronic data by law enforcement authorities. (CR)

#### EDPS Annual Report 2024

On 23 April 2025, the European Data Protection Supervisor (EDPS) presented its [Annual Report 2024](#), which reviews activities over the year organised under the headings of supervision and enforcement, policy and consultation, technology and privacy, and artificial intelligence.

The year 2024 was marked by celebrations around the 20th anniversary of the EDPS. ([→eucrim 2/2024, 107](#)). On this occasion, the EDPS published a book entitled “Two Decades of Personal Data Protection: What Next?”, retracing its journey, highlighting its role in shaping the digital landscape and safeguarding privacy, reflecting on key lessons learned, and anticipating future challenges. The EDPS also launched the [20 Talks](#) series, exploring the role of privacy and data protection across various sectors, bringing together experts from technology, policy, academia, and activism.

Throughout the year, the EDPS worked on [20 initiatives](#), publishing one per month, to keep pace with the evolving digital landscape and to strengthen its position as a modern data protection authority. In June 2024, a major conference in Brussels marked EDPS’s anniversary, drawing data protection specialists, policymakers, and technology experts to reflect on the role of data protection in modern democracies.

Alongside its anniversary events, the EDPS introduced several new initiatives in 2024, including the creation of an Artificial Intelligence Unit and the launch of an AI Strategy centred on governance, risk management, and supervision. It also provided a record-breaking 97 responses to legislative consultation requests from the Eu-

European Commission, issuing opinions and formal and informal comments to guide data protection in draft EU legislation and international agreements.

In the area of Justice and Home Affairs, the EDPS issued Opinions on, for example:

- The proposed Regulation to extend the temporary derogation from certain ePrivacy Directive provisions to combat child sexual abuse online;
- The Regulation to enhance police cooperation to prevent, detect, and investigate the smuggling of migrants and the trafficking of human beings, and to reinforce the role of Europol in preventing and combating these crimes;
- Proposed agreements to enhance judicial cooperation with Eurojust and Bosnia & Herzegovina and the Republic of Lebanon;
- The EU–Canada agreement on transfers of Passenger Name Record (PNR) data.

The EDPS also closely followed the development and interoperability of the EU's large-scale IT systems to support law enforcement, border management, and migration and asylum. Such systems include the Entry/Exit System (EES), Visa Information System (VIS), European Travel Information and Authorisation System (ETIAS), Eurodac, Schengen Information System (SIS), and the European Criminal Records Information System for Third Country Nationals (ECRIS TCN).

In its capacity as supervisory authority, the EDPS reprimanded Frontex for failing to comply with its regulation when transmitting personal data of cross-border crime suspects to Europol. ([→eucrim 4/2024, 280–281](#)). It also issued 23 recommendations to Europol to ensure or improve its compliance with the data protection legal framework.

Finally, the year 2024 marked the conclusion of the [EDPS Strategy 2020–2024](#) focused on building a safer, fairer, and more sustainable digital

Europe ([→eucrim 2/2020, 102](#)). To this end, the EDPS published a review of its mandate during this period ([→separate news item](#)). (CR)

### European Public Prosecutor's Office (EPPO)

#### ECJ Judgment on Judicial Review of Acts of EDPs



In its [judgement](#) of 8 April 2025 in [Case C-292/23](#) (*Criminal proceedings against I.R.O. and F.J.L.R.*), the European Court of Justice (ECJ) examined the compatibility with the EPPO Regulation of national law restricting the judicial review of procedural acts of European Delegated Prosecutors (EDPs) only to a list of acts exempting, above all, witness summons. According to the ECJ, procedural acts of the EPPO capable of affecting the legal situation of the persons challenging them must be amenable to judicial review. It is, however, for the national court – by means of a concrete and specific examination – to determine whether or not this is the case.

#### ► [Background of the case and question referred](#)

The request for a preliminary ruling stems from criminal proceedings in Spain where two suspects were under investigation by the EPPO for subsidy fraud and forgery of documents related to EU project financing. The Spanish EDPs handling the case had summoned two individuals to give evidence. The suspects, I.R.O. and F.J.L.R., challenged the summons issued for one of the witnesses to appear. They argued that this investigative measure (witness questioning by the EDP) was neither relevant, necessary, nor useful, since the witness had already been heard in a previous investigation into the matter triggered by OLAF (before the EPPO exercised its right of evocation). After the EPPO dismissed their appeal against the

witness summons, the defendants wished to appeal before the referring court (the Juzgado Central de Instrucción no 6 de Madrid (Central Court of Preliminary Investigation No 6, Madrid, Spain)).

The Madrid court indicated, however, that Spanish law only permits judicial review of EPPO procedural acts in cases expressly provided for by the law implementing enhanced cooperation on the establishment of the EPPO, not listing, for instance, witness summons. It did, however, consider the act capable of producing legal effects with regard to third parties and therefore concluded that judicial review provided for by EU law should be possible for this type of act, in order to avoid unjustified restrictions on EU-derived rights. The referring court also saw an issue of equivalence, since, in criminal proceedings conducted in Spain by the investigative judge, the Code of Criminal Procedure does not lay down any kind of limitation as to the possibility of challenging decisions of the investigating judge on carrying out or refusing investigation measures.

Hence, the referring court asked, in essence, whether Art. 42(1) of [Regulation 2017/1939](#), read in the light of the second subparagraph of Art. 19(1) TEU, Arts. 47 and 48 of the Charter of Fundamental Rights and the principles of equivalence and effectiveness, must be interpreted as precluding national legislation pursuant to which persons who are the subject of an EPPO investigation may not directly challenge before the competent national court a decision by which, in the context of that investigation, the European Delegated Prosecutor handling the case concerned summons witnesses to appear.

#### ► [Ruling of the ECJ \(Grand Chamber\)](#)

In its judgement, the ECJ (sitting as Grand Chamber) first examined the meaning of the legal notions in Art. 42(1) of EPPO Regulation

2017/1939, which provides that “[p]rocedural acts of the EPPO that are intended to produce legal effects vis-à-vis third parties shall be subject to review by the competent national courts (...)”. The Court noted that the concept of “procedural acts of the EPPO that are intended to produce legal effects vis-à-vis third parties”, within the meaning of Art. 42(1), is an autonomous concept of EU law that must be interpreted on the basis of uniform criteria:

■ “Procedural acts” includes, in particular, those acts “undertaken by the EPPO in the course of its investigations”. This is the case for witness summons.

■ The expression “intended to produce legal effects vis-à-vis third parties” corresponds to the criterion used in the first paragraph of Art. 263 TFEU to define the scope of acts that may be challenged before the EU Courts by way of an action for annulment. This means that judicial review covers all acts of a procedural nature intended to produce binding legal effects capable of affecting the interests of third parties by bringing about a distinct change in their legal position.

According to the judges in Luxembourg, it is for the national court to assess *in concreto* whether the decision of a European Delegated Prosecutor to summon a witness is intended to produce said effects. The national court must take into account the “third party” status of the person challenging the act, the content of the act, the context within which it was adopted, and the powers of the body that ordered it. The ECJ also clarified that national procedural rules as well as the specific context of the criminal investigation in which the EPPO adopted said decision play a role. In this context, the EU legislature wished to limit review of EPPO acts “to that which is strictly necessary to ensure, in respect of those acts, a uniform level of effective judicial protection which complies with EU primary law.”

If the referring court comes to the conclusion that the witness summons fulfils the criteria of Art. 42(1) of the EPPO Regulation, the ECJ further ruled that national law must guarantee these persons an effective judicial review of that decision by the criminal trial court, at least as an incidental question, where applicable. However, the principle of equivalence requires that, if national procedural rules allow for the direct challenge of comparable domestic decisions, the same opportunity must be available to individuals challenging analogous decisions under EU law.

#### ► Put in focus

The ECJ’s judgment of 8 April 2025 in Case C-292/23 is the second important ruling on interpretation of the EPPO Regulation 2017/1939 following a request for preliminary ruling. The first judgment (Case C-281/22, G.K. and Others) was delivered in December 2023 and concerned the extent of judicial review in a Member State assisting an EDP handling an EPPO case in cross-border investigations (→news in [eucrim 4/2023, 319–321](#) and the articles by *Hans-Holger Herrnfeld* in [eucrim 4/2023, 370–380](#) and *Katalin Ligeti* in [eucrim 1/2024, 69–76](#)). The present case again concerned the topic of judicial review – this time within the jurisdiction of the EDP handling the case.

In short, the ECJ first emphasised that even “formally harmless” procedural acts of the EPPO may be subject to judicial review. This is, however, only the case if the act has legal significance and review must thus be given in the context of safeguarding the rights of defence. It is now up to the competent national court to apply the criteria established by the ECJ. The lengthy reasoning about the concept and interpretation of “a procedural act that intends to produce legal effects vis-à-vis third parties” pursuant to Art. 42(1) of the EPPO Regulation, as well as several other hints in the

judgment, indicate that the Court itself is not fully convinced that the requirements in favour of judicial review under Art. 42(1) have been met in the present case (witness summons). Nonetheless, the judgment provided the judges in Luxembourg with the opportunity to give guidance on Art. 42 of the EPPO Regulation and to draw the limits of defence rights with regard to judicial reviews.

Secondly, the ECJ made clear that, if judicial review is considered necessary, this does not necessarily mean that a direct and specific legal remedy must be available for such review. The review may also be carried out incidentally in subsequent proceedings, provided that the right to an effective remedy and to a fair trial, as well as the presumption of innocence and the rights of the defence, are safeguarded. However, in the case of a direct remedy to directly challenge a decision taken by the national authorities, the same possibility must also exist in relation to actions of the European Public Prosecutor’s Office. It will be interesting to see how the referring Spanish court will implement the guidance from Luxembourg and assess the compatibility of the Spanish law implementing the EPPO Regulation with the EU standards. (CR/TW)

#### Call for Applications Launched for Successor to Laura Kövesi

According to Art. 14(1) of the EPPO Regulation, the European Chief Prosecutor is appointed for a non-renewable term of seven years. As the current term of the European Chief Prosecutor *Laura Kövesi* is nearing its end on 31 October 2026, the Commission has [published an open call](#) for candidates for the position in the Official Journal of the EU on 28 April 2025.

The European Chief Prosecutor leads the EPPO in organising its work, directing its activities, and taking decisions in accordance with the EPPO Regulation and the internal rules of



procedure of the EPPO. He/she represents the EPPO vis-à-vis the institutions of the Union and of the Member States of the European Union and third parties. The European Chief Prosecutor also has other duties and responsibilities in accordance with the EPPO Regulation, e.g.:

- Making a proposal to the College of the EPPO for appointments to the position of European Delegated Prosecutor and to the position of Administrative Director of the EPPO;
- Taking part in and chairing the meetings of the Permanent Chambers in accordance with the internal rules of procedure of the EPPO;
- Preparing and chairing regular meetings of the College of the EPPO;
- Preparing estimates of the revenue and expenditure of the EPPO for each financial year, corresponding to the calendar year, on the basis of a proposal drawn up by the Administrative Director;
- Making proposals for implementing rules and programme documents for adoption by the College;
- Meeting on a regular basis with the President of Eurojust to discuss issues of common concern and, where appropriate, participating in the meetings of the College of Eurojust;
- Meeting on a regular basis with the heads of other relevant EU bodies, offices, and agencies, such as Europol and OLAF, and relevant networks of Union agencies;
- Carrying out any other task, as provided in the EPPO Regulation, the Decisions of the College, and the internal rules of procedure of the EPPO.

To be considered for the selection phase, candidates must meet several minimum requirements, for instance holding citizenship of one of the EU Member States participating in the enhanced cooperation on the establishment of the EPPO. Another eligibility criteria is for instance that the candidates possess the qualifications required for appointment to the highest

prosecutorial or judicial offices in their respective Member States and have relevant practical experience of national legal systems, financial investigations and of international judicial cooperation in criminal matters, obtained at domestic, European or international level, or have served as European Prosecutors. Following the selection procedure, the European Chief Prosecutor is appointed by the European Parliament and the Council by common accord. (CR)

### Publication of EPPO's Annual Report 2024

On 3 March 2025, the European Public Prosecutor's Office (EPPO) published its [Annual Report for the year 2024](#). The report gives an overview of the EPPO's operational activities and the activities of its College, permanent Chambers, and European Delegated Prosecutors.

Key figures for the year 2024 are as follows:

- The number of active investigations by the EPPO increased to a total of 2666 active investigations compared to 1927 in 2023;
- The damage to the EU budget is estimated at €24.8 billion compared to €19.2 billion in 2023;
- The EPPO opened 1500 new investigations in 2024 (10% more than in 2023);
- The EPPO was handling 311 active cases related to NextGenerationEU (compared to 206 in 2022), the majority of which stemmed from the Recovery and Resilience Facility (RRF). The estimated damage to the EU's financial interests amounts to €2.8 billion, which represents 30% of the total estimated damage for subsidy fraud.
- The EPPO received and processed 6547 crime reports (56% more than in 2023); 70% came from private parties and almost 27% from national authorities, while only 1.7% came from EU institutions, bodies, offices, and agencies;

- VAT fraud accounted for 53% of the overall damage with an estimated damage of €13.15 billion;

- The EPPO filed 205 indictments compared to 139 in 2023, bringing more perpetrators of EU fraud to judgment before national courts;

- National judges granted European Delegated Prosecutors freezing orders worth €2.42 billion.

Looking at these numbers, the report concludes that the level of detecting fraud affecting the EU's financial interests in the participating Member States has further improved. Public awareness about the EPPO has increased, but there was still no improvement in terms of detection and reporting on the part of EU institutions, bodies, offices, and agencies.

The majority of investigated offences identified in active EPPO cases concern non-procurement expenditure fraud (2105), VAT revenue fraud (1287), and inextricably linked offences (808). Next in line are offences such as non-VAT revenue fraud, procurement expenditure fraud, money laundering, PIF-crime focused criminal organisation, corruption, and misappropriation.

As in the previous year, most of the active funding fraud investigations concerned agricultural and rural development programmes as well as regional and urban development programmes. Investigations also took place, however, for programmes involving recovery and resilience, employment, social cohesion, inclusion and values, maritime and fisheries, research and innovation, international cooperation, education and culture, mobility, transport, energy, digitalisation, asylum, migration, integration, industry and entrepreneurship, climate and environment, and security and defence.

Alongside the general overview, the annual report analyses the operational activity, relevant judicial activity, typologies of identified active EPPO cases,



and active fraud investigations for each of the 24 Member States participating in the EPPO in 2024. In terms of relations with non-participating Member States and non-EU countries in 2024, the most important step was that Poland and Sweden acceded the EPPO.

Lastly, the annual report provides an overview on IT, security, corporate services, staff development, human resources, transparency, relations with the general public and the press, activities of the legal service, data protection, and financial resources (with a budget of €76.4 million for delivery of the EPPO's mission in 2024). (CR)

## Specific Areas of Crime

### Protection of Financial Interests

#### Commission Launched Preparations for Financial Framework 2028+

On 12 February 2025, the European Commission presented a [Communication which directs the road to the next multiannual financial framework](#) (MFF). The next MFF will start in 2028 and will cover at least five years. The Communication outlines some of the key policy and budgetary challenges for the next MFF. It is designed to be the basis for a broad dialogue to prepare the respective budget proposal. Therefore, the Commission launched in parallel a [portal](#) via which European citizens can share their views to help define the future EU budget as well as a [“European Citizens’ Panel”](#), in which 150 randomly selected European citizens will work together with the Commission to formulate concrete recommendations on “a new European budget fit for our ambition”.

Given the scale of challenges ahead, such as remaining barriers within the single market, rising security threats, and persistent difficulties with regard to Europe's sustainability, the Commission

calls for an ambitious budget, both in size and design. The Commission describes five strands that should guide “Europe's choice” for the next MFF:

- A more focused EU budget;
- A simpler EU budget;
- An EU budget with greater impact;
- A more flexible EU budget;
- A budget that delivers on EU priorities.

Looking at the financing of the next EU budget, the Commission calls for modernising the revenue side and advocates the introduction of new own resources. The status quo – with stable national contributions – is no option. The Commission calls on the Council to resume work on the issue of new own resources as a matter of urgency, in line with the Interinstitutional Agreement from 2020 and the [Budapest Declaration on the New European Competitiveness Deal](#). Further ideas of the Commission for the MFF 2028+ include the following:

- Agreeing on a new approach for a modern EU budget with a plan for each country with key reforms and investments, designed and implemented in partnership with national, regional, and local authorities;
- Establishing a European Competitiveness Fund to support strategic sectors and critical technologies;
- Revamping external action financing which must become more impactful, targeted and aligned with strategic interests;
- Providing additional safeguards for the protection of the rule of law.

Next steps: After consultation with the European citizens and a [Tour d'Europe](#) by Commissioner for Budget *Piotr Sieraffin*, the Commission plans to present a formal proposal for the next MFF in July 2025. A timely agreement before its implementation in January 2028 is envisaged. The MFF must be adopted by unanimity by the 27 EU Member States in the Council, after obtaining the consent of the European Parliament. (TW)

### EP Set Out its Priorities for 2026 Budget

On 2 April 2025, the plenary of the European Parliament (EP) adopted the [Parliament's guidelines for the 2026 EU budget](#). The guidelines are designed to set out the EP's expectations towards the Commission when drafting its budget proposal (expected in June 2025). MEPs wish that the 2026 EU budget bolsters EU defence and security capabilities. The budget should focus on strategic preparedness and security, economic competitiveness and resilience, sustainability, climate, and the single market. The EU should also arrange additional investments in research, innovation, enterprises, health, energy, migration, border protection, digital and green transitions, job creation and opportunities for young people.

MEPs call for improved EU security, cybersecurity and defence capabilities, and funding for dual-use transport infrastructure. Another important issue for the MEPs is the proper use of EU funds while upholding the rule of law. It is also emphasised that repayment of the borrowing costs of the NextGenerationEU recovery plan must not lead to a reduction in EU programmes and funds. (TW)

### New Legal Framework for Commission's Chief Risk Officer

On 21 February 2025, the European Commission adopted [Decision 2025/369](#) expanding the role of the Chief Risk Officer (CRO). The new legal framework for the Commission's CRO reacts to the increasing and more complex financial instruments that leverage the EU budget over the past years. It implements the recommendations of the European Court of Auditors' special report 16/2023 on EU debt management. The CRO acts independently, with an oversight over now all of the Union's financial operations:

- Borrowing, debt, and liquidity management;

- Lending operations and budgetary guarantees;
- Asset management.

Operating independently from other Commission services responsible for financial operations, the function of the CRO can be seen as a central pillar of the “three lines of defence” model, a best-practice framework for risk governance:

- The first line of defence consists of the Commission departments managing EU borrowing, lending, and asset management operations as well as budgetary guarantees.
- As an independent, corporate, second line of defence, the CRO formulates risk management policies and provides independent risk oversight, ensuring additional controls and accountability.
- The third line of defence is the Internal Audit Service, providing independent assurance on risk governance.

The CRO was established in 2021 and its position is held by *Iliyana Tzanova*. The new Commissioner for Budget, Anti-Fraud and Public Administration, [Piotr Serafin](#), said:

“Strengthening the role of the Chief Risk Officer is a testament to the EU’s commitment to maintaining high standards of financial risk oversight. The use of loans and budgetary guarantees will remain an essential instrument to drive the EU’s political priorities and support investments for climate transition, competitiveness and external action. As we navigate an increasingly complex financial landscape, these measures ensure that the EU remains prepared to address emerging challenges with robust risk management practices.” (CR)

#### **ECA: Weak Compliance with Public Procurement and State Aid Rules for Money Spent under the RRF**

The European Commission still cannot be certain that EU countries have effective systems to ensure that the EU’s €650 billion Recovery and Resilience Facility (RRF) complies with public procurement and state aid rules.

This is the main message of the European Court of Auditor’s (ECA) [special report 09/2025](#) entitled: “Systems for ensuring compliance of RRF spending with public procurement and state aid rules – Improving but still insufficient”. The report was published on 10 March 2025 and complements previous reports on the control system of the RRF (the EU’s new funding model to overcome the negative effects of the COVID-19 pandemic), such as the special report 07/2023 on the design of the Commission’s control system for the RRF ([→eucrim 1/2023, 25–26](#)) and special report 22/2024 on the risk of double funding from the EU budget ([→eucrim 3/2024, 185](#)).

For the present report, the ECA assessed the RRF control systems at Commission and EU Member State level, asking as to whether the Commission has been able to draw sufficient assurance that Member State internal control systems are effective in ensuring that RRF-funded measures complied with public procurement and state aid rules.

ECA’s auditors found that EU countries had weaknesses when it came to checking public procurement compliance. Problems have existed in relation to the coverage, quality and/or timing of checks. As far as state aid is concerned, national RRF audit bodies generally had no assurance on state aid when payment requests were submitted. A main issue resulting in the detected shortcomings are unclear rules, as EU countries were given no detailed guidance on how to check EU public procurement and state aid rules. Although the Commission has improved its audit strategy since the initial phase of RRF implementation, ECA’s auditors still found problems. For instance, not all EU countries that received RRF funding were checked with the same degree of detail for public procurement control and audit sys-

tems. Another issue are shortcomings in the recovery of misspent EU money, which, as the report stresses, is also due to the design of the RRF where payments are solely based on the satisfactory fulfilment of milestones and targets.

Based on its findings, the ECA provides several recommendations for the Commission to ensure compliance with public procurement and state aid rules and improve control and audit systems in this area. (TW)

#### **ECA: EU Money Granted to NGOs Still Not Transparent**

On 7 April 2025, the European Court of Auditors (ECA) published its [special report no 11/2025](#) in which it examined the transparency of EU funding granted to non-governmental organisations (NGOs) in EU internal policies.

The ECA highlighted that, in the audited period 2021–2023, over 12,000 NGOs received money from the EU internal policy programmes (e.g., cohesion, research, migration and the environment) amounting to €7.4 billion. Over the past decade, a substantial part of the Commission’s direct funding went to a small number of NGOs. ECA’s auditors doubt, however, whether these figures are fully correct as a reliable overview is lacking. The information is published in a fragmented way, which hampers transparency, impedes analysis of whether EU funds are overly concentrated on a small number of NGOs, and restricts insight into the role of NGOs in EU policies. Other shortcomings found are, *inter alia*:

- Disclosure of information is insufficient, and Member States do not monitor or report on the EU funding granted to NGOs;
- The definition of “NGO” is unclear and varies at the EU and Member State levels; thus it cannot be ensured that NGO’s are correctly classified in the EU’s financial transparency system. In



addition, there are no checks on important aspects of the NGOs' status;

- The Commission did not properly disclose certain EU-funded advocacy activities such as lobbying;
- EU fund managers do not proactively search for potential NGO breaches of EU values, such as the rule of law and human rights, but rely mainly on self-declarations.

Against this background, the ECA recommends that the Commission should do the following:

- Improve guidance on classifying non-governmental organisations;
- Improve the quality of information on EU spending in the financial transparency system;
- Strengthen verification of compliance with EU values.

ECA's special report no 11/2025 was drafted against the background of calls by the European Parliament to strengthen transparency and accountability of EU funding granted to recipients, including NGOs, as a consequence of the 2022 "Qatargate" scandal ([→eucrim 4/2022, 242–243](#)). The present ECA report follows the ECA's 2018 [audit report](#) on EU funding granted to NGOs in external action policy and the 2024 [special report](#) on the EU's transparency register. The ECA states that only minor improvements have been made compared to its 2018 audit. (TW)

### European Chief Prosecutor Raises Concerns about Changes to Austrian Criminal Procedure Law

New amendments to the Austrian law on criminal procedure entered into force on 1 January 2025. In addition, the Austrian Federal Ministry of Justice presented a draft for an Act on the implementation of EU Criminal Justice Acts. In light of these legislative amendments and the draft Act, the European Chief Prosecutor *Laura Codruța Kövesi* sent a [formal letter](#) to the European Commission on 23 January 2025 expressing her concerns.

According to Kövesi, the amendments to the Austrian law on criminal procedure cannot be reconciled with the principles of the rule of law as laid down in Regulation (EU) 2020/2092 on a general regime of conditionality for the protection of the budget of the EU (Conditionality Regulation [→eucrim 2020, 174–176](#)). She criticises that the new legislation makes the collection and seizure of digital evidence ex-

tremely difficult, if not impossible, for the prosecution services, including the EPPO, when acting in Austria.

With regard to the draft Act on the implementation of EU Criminal Justice Acts, Kövesi is worried that the draft law does not remedy some of the most obvious shortcomings of the adaptation of the Austrian legal system to the EPPO Regulation. It also contains draft provisions, which raise further serious

## Money Laundering

### Guidance on Cooperation between Financial Institutions and Investigative Authorities

The Europol Financial Intelligence Public Private Partnership (EFIPPP) is a collaborative mechanism for more than 90 private stakeholders, Financial Intelligence Units (FIUs), and law enforcement agencies to address threat information across the community in a structured way. The EFIPPP secretariat is located within the European Financial and Economic Crime Centre (EFECC) at Europol.

At the end of January 2025, the EFIPPP published a [practical guide](#) with an overview of how and why to ensure successful operational cooperation between financial institutions and investigative authorities in the fight against financial crime.

The guide also aims to raise awareness among policymakers and relevant authorities about the added value of public-private cooperation. It outlines the objectives, benefits, methods, and conditions for cooperation as well as the key factors of an effective legal framework. Looking at the benefits of cooperation, there is added value for both investigative authorities and financial institutions, for example the building of synergies between investigative authorities and private sector compliance.

The guide underlines three objectives of the cooperation that are particularly notable from the perspective of investigative authorities:

- To identify new investigative leads to trigger or guide investigations;
- To support the gathering of evidence in support of ongoing investigations;
- To disrupt a specific threat through preventive measures.

Lastly, the guide highlights some basic conditions that are key to this cooperation, such as commitment, trust, a willingness to innovate, robust processes to maintain the integrity of investigations, and inter-agency agreement. It concludes with some general rules drawn from past experience, in addition to giving detailed guidance on methods and scenarios for cooperation between investigating authorities and financial institutions.

*Background:* The Guide is the outcome of the work of the EFIPPP Legal Gateways Working Group, and was drafted by Dr. *Benjamin Vogel*, drawing on his scientific work on AML/CFT and public-private information sharing conducted at the Max Planck Institute for the Study of Crime, Security and Law since 2014 ([→see also: B. Vogel and M. Lassalle, "Developing Public-Private Information Sharing to Strengthen the Fight Against Money Laundering and Terrorism Financing", \*eucrim\* 4/2023, 384–392](#)). (CR)

concerns, in particular as regards the intrusive supervision powers of a non-judicial authority, and, ultimately, as regards respect for the EPPO's independence.

Accordingly, on the basis of Recital 16 of the Conditionality Regulation, the European Chief Prosecutor informed the European Commission that the new provisions already in place, as well as those under discussion, threaten the effectiveness and efficiency of the EPPO's investigations under Austrian law, as they create a situation in which a national, non-judicial authority is in a position to interfere with such investigations. It is anticipated that the European Commission will examine the concerns raised by the EPPO and that further action may be taken.

In a statement published in June 2024, Kövesi already criticised the proposed amendments to the Austrian Code of Criminal Procedure after a judgment of the Austrian Constitutional Court that called for stricter rules on seizure of data and data storage on devices ([→eucrim 2/2024, 102](#)). (CR)

## Tax Evasion

### DAC9: New Rules on Minimum Effective Corporate Taxation

On 14 April 2025, the Council of the European Union [adopted](#) a Directive amending Directive 2011/16/EU on administrative cooperation in the field of taxation (DAC 9). The Directive was published in the [Official Journal L 2025/872 of 6 May 2025](#).

It extends cooperation and information exchange in the area of effective minimum taxation of companies and implements specific provisions from "Pillar 2" of the G20/OECD global agreement on international tax reform. The aim is to limit the race to the bottom in corporate tax rates, reduce the risk of tax base erosion and profit shifting, and ensure that the largest multinational companies pay the

agreed global minimum corporate tax rate. The [Pillar 2 Directive](#) ensures that profits of the largest multinational and domestic groups or companies (with a combined annual group turnover of at least €750 million) are taxed at a minimum effective rate of 15%.

DAC9 also simplifies reporting and disclosure requirements for large companies by allowing the bundled, centralised filing of a top-up tax information return for the entire group concerned (instead of a multiple filing being made by each constituent entity of an enterprise group at local level). Thus, DAC9 contributes to the EU's efforts to rationalise reporting obligations and to reduce burden on EU businesses.

Finally, the Directive extends the framework for automatic exchange between EU Member States to the top-up tax information return.

Member States must transpose the Directive into national law by 31 December 2025. Multinational enterprise groups are expected to file their first top-up tax information return by 30 June 2026, as required under the Pillar 2 Directive. The relevant tax authorities must exchange this information with each other by 31 December 2026 at the latest. (TW)

### New Legislation: VAT in the Digital Age

On 11 March 2025, the [Council adopted](#) a legislative package that makes the existing EU rules on value added tax (VAT) fit for the digital age. The package consists of the following legislative acts which were published in the EU's [Official Journal of 25 March 2025](#):

- Council [Directive \(EU\) 2025/516](#) amending Directive 2006/112/EC as regards VAT rules for the digital age;

- Council [Regulation \(EU\) 2025/517](#) amending Regulation (EU) No 904/2010 as regards the VAT administrative cooperation arrangements needed for the digital age;

- Council [Implementing Regulation \(EU\) 2025/518](#) amending Implementing Regulation (EU) No 282/2011 as regards information requirements for certain VAT schemes.

The new rules will not only introduce several measures for the digitalisation in the field of VAT but also aim at fighting VAT evasion and avoidance more effectively. For the Commission proposal [→eucrim 4/2022, 246–247](#).

The **Directive** makes digital VAT reporting by companies who sell goods and services to businesses in another EU Member State obligatory by 2030. The transactions to be reported to tax administrations will be documented electronically and the use of electronic invoicing will become the default system for issuing invoices. The amending Directive clarifies the European standard on electronic invoices and harmonises the information required for electronic transmission of VAT documents to the tax administrations. With a view to ensuring a more effective fight against fraud, Member States will be allowed to provide that holding an electronic invoice issued in compliance with the required European standard is a substantive condition for entitlement to deduct or reclaim the VAT due or paid.

The Directive also introduces the "deemed supplier" model for online platforms active in short-term accommodation rental and passenger transport by road, i.e., platforms will be required to charge VAT where underlying suppliers do not charge VAT because they are, for example, non-taxable persons or taxable persons availing themselves of the special scheme for small enterprises.

Last but not least, in order to support the objective of a single VAT registration in the Union, the Directive improves and expands online VAT one-stop-shops (OSS) so that businesses do not have to go through costly registrations for VAT in every EU Member State in which they do business.



The amending **Regulation** complements the VAT Directive and, in essence, lays down the rules for the establishment of an electronic central VAT information exchange system (“central VIES”) for sharing VAT information. This system is expected to be an important measure to fight VAT fraud. Member States must automatically transmit VAT information to the central VIES. Eurofisc liaison officials of Member States will have direct access to the central VIES.

The **Implementing Regulation** specifies certain elements of the “deemed supplier” rule with regard to electronic interfaces such as marketplaces, platforms, portals or similar means that facilitate the supply of short-term accommodation rental services or passenger transport services by road. (TW)

#### ECA: Simplified EU Customs Procedures Vulnerable to VAT Fraud

The European Court of Auditors (ECA) believes that simplified import customs procedures in the EU are vulnerable to VAT fraud. Existing measures are not sufficient to prevent and detect VAT import fraud when such procedures are used. In their [special report 08/2025](#) “Value Added Tax fraud on imports – The EU’s financial interests are insufficiently protected under simplified import customs procedures”, ECA’s auditors therefore warn of considerable risks of abuse. The report was published on 24 March 2025.

In particular, the ECA identified gaps and inconsistencies in the EU legal framework and serious shortcomings in the way Member States check that the correct amount of VAT is collected. Many of these shortcomings are due to the challenges faced by customs and tax authorities in cooperating between Member States. The ECA recommends that the Commission propose changes to the legal framework to achieve a more uniform application

#### Study Makes Proposals for Combating Tax Avoidance on Capital Gains

At the beginning of February 2025, the Foundation for European Progressive Studies (FEPS) in Belgium and the Kalevi Sorsa Foundation in Finland published a [study on “tackling tax avoidance – reforming capital income taxation in the EU”](#). Financially supported by the European Parliament, the study aims to contribute to recent discussion on better international tax cooperation and harmonisation of capital income taxation of individuals. It identifies loopholes and asymmetries of national capital income tax regimes in 15 selected European countries, with the objective to discuss how capital income taxation should be harmonised and further developed in the EU. The study describes the role of capital income taxation in the tax system, analyses the current problems of capital income taxation, and presents case studies on the 15 different European tax regimes.

According to the study, most of the 15 European countries surveyed offer significant tax advantages to wealthy individuals. An increasing number of states have also created tax breaks specifically for people who move abroad. At the same time, tax evasion on capital income is increasing significantly because existing bilateral tax treaties are insufficient to effectively protect tax bases. The study presents five essential tax policy recommendations that would tackle capital income tax base erosion and tax avoidance as addressed in the study. Hence, the EU should do the following:

- Adopt a directive establishing a minimum capital income tax rate;
- Adopt an anti-tax avoidance directive (ATAD) for capital income (similar to the current ATAD for corporate income tax), including an exit tax rule for individuals;
- Adopt a directive to tax unrealised capital gains which would avoid that income might never be taxed and which ensures that high-net-worth individuals are effectively taxed;
- Extend the scope the EU Code of Conduct on Business Taxation to include capital income taxation.

Furthermore, the authors of the study recommend that the minimum capital income tax rate be complemented with net wealth taxes on the ultra-rich. Net wealth taxes on high-net-worth individuals would be efficient in tackling wealth concentration and increase the transparency of wealth. (TW)

of simplified customs procedures at import in the different Member States, analyse the benefits of a requirement for mandatory transport evidence for consignments under customs procedure 42 and require more effective cooperation between national customs and tax authorities.

In its response to the report, the [Commission welcomed the recommendations](#) and stressed that it is committed to working closely with Member States to implement these measures and to continue monitoring and analysing the regulatory framework and its implementation. (TW)

#### Counterfeiting & Piracy

##### Europol Report: Pharmaceutical Crime in the EU

**spot light** At the end of January 2025, Europol published a new [report](#) outlining its assessment of the threat posed by pharmaceutical crime in the EU and beyond – an illicit market that is global and growing. The report aims to raise awareness of how criminal networks exploit consumers and industry to generate illegal revenues through the production and sale of counterfeit medicines as well as substandard, falsified, and counterfeit



health products. Forms of crime include the following:

- *Substandard health products* come from legitimate manufacturers but do not meet quality standards.

- *Counterfeit health products* are medicines that deliberately misrepresent their identity, composition, or source. They can include products with incorrect ingredients, the wrong amount of the correct ingredients, no active ingredients, or fake packaging. The intention behind counterfeit products is to deceive consumers about their origin and efficacy. Counterfeit drugs may look identical to the real product, which is why they are classified as a subset of falsified products.

- *Falsified health products* typically involve unauthorised replication of brand-name medicines.

While all counterfeit drugs can be considered falsified, not all substandard or falsified products are counterfeit. Nevertheless, each category poses a significant risk to public health and generates enormous financial losses for legitimate companies, undermines brand credibility, and also endangers investments in research.

According to the report, criminal actors and networks operating in the EU are involved in either importing, exporting, or manufacturing such illicit products. They target a wide range of products. Diversion from the legitimate supply chain, through illicit acquisition via counterfeit or stolen prescriptions, or through legitimate sales, is a common modus operandi driven by market needs, the value of medicines, and legal supply challenges. Social media and online marketplaces, both on the surface and on the dark web, remain central to the trade in counterfeit pharmaceuticals.

The misuse of prescription and over-the-counter medicines as well as other health products for recreational purposes, psychoactive effects, weight loss, performance enhancement and/or cosmetics also continues

to remain a widespread and growing phenomenon. This increasing demand will generate continuous opportunities for organised crime.

Lastly, the report emphasises the need for a multidisciplinary approach to tackling pharmaceutical crime, involving all key stakeholders such as law enforcement, health authorities, patent holders, the manufacturing industry, and digital service providers. (CR)

## Cybercrime

### Europol & Eurojust Publish New Edition of Cybercrime Report

On 31 January 2025, Europol and Eurojust published a [new edition](#) of their joint report on the common challenges that law enforcement and the judiciary face in the fight against cybercrime. The 2024 edition also offers a new, second part focusing on legal instruments that could mitigate some of these challenges. The first joint report was published in September 2019 ([→eucrim 2/2019, 98](#)).

Common challenges include data volume, loss of data, access to data, anonymisation services, obstacles to international cooperation, and hurdles in public-private partnerships. The report also discusses legislative means to tackle cybercrime, including options under the e-Evidence Package (European Production and Preservation Orders), the Digital Services Act Regulation, the EU's Artificial Intelligence Act, the Second Additional Protocol to the Budapest Convention on Cybercrime, and the CLOUD Act. It also analyses developments regarding the Executive Agreement between the EU and the USA.

Given the growing challenges of the unavailability of data in criminal investigations – due to technological developments and lack of data retention, jurisdictional barriers, and the complications inherent in public-private part-

nerships –, the report calls for a nuanced approach that balances strong security measures with the protection of individual privacy and civil liberties.

The report concludes that the realm of cybercrime is not static but an ever-evolving battleground where new challenges and solutions continually emerge. With regard to the new legislative tools, the report underscores that the real test lies in the practical application of these tools and the seamless integration into existing frameworks that will make them fully effective. (CR)

### Cybercrime Forums “Cracked” and “Nulled” Taken Down

The world's two largest cybercrime forums, [“Cracked.io”](#) and [“Nulled.io”](#), were taken down at the end of January 2025. The law enforcement operation that was led by German authorities and supported by Europol involved eight countries from Europe, the United States, and Australia.

The two sites worked as one-stop shops and were used not only to discuss cybercrime but also to serve as marketplaces for illegal goods and cybercrime-as-a-service, such as stolen data, malware, or hacking tools. They also offered AI-based tools and scripts to automatically scan for security vulnerabilities and optimise attacks. It is estimated that the suspects made €1 million in criminal profits.

As a result of the action days, two suspects were arrested; seven properties searched; and 17 servers, over 50 electronic devices, and around €300,000 in cash and cryptocurrencies seized. (CR)

### Hit against AI-Generated Child Sexual Abuse Material

At the end of February 2025, a global operation against the sexual exploitation of children led to 25 arrests. [“Operation Cumberland”](#), conducted by 19 countries and supported by Europol, is one of the first cases involving ar-

tificially generated child sexual abuse material (CSAM). This crime is particularly challenging because national legislation to deal with it is lacking.

Even in cases in which the content is fully artificial and there is no real victim depicted, AI-generated CSAM still contributes to the objectification and sexualisation of children. Authorities face significant challenges in identifying real victims in the face of AI-generated CSAM. These crimes therefore require both new investigative methods and tools for law enforcement and, in addition, corresponding new legislation. In this context, EU Member States are currently discussing a common [Regulation](#) proposed by the European Commission to address this new situation and protect children from sexual abuse and exploitation ([→eucrim 2/2022, 91–92](#)). (CR)

### Pedophile Platform “Kidflix” Shut Down

In an international operation against child sexual exploitation, one of the world’s largest paedophile platforms was shut down at the beginning of April 2025. Between April 2022 and March 2025, a total of 1.8 million users worldwide had logged on to the [Kidflix](#) platform, which contained around 91,000 videos uploaded and shared by users.

Through “Operation Stream”, largely supported by Europol and involving 35 countries, almost 1400 suspects were able to be identified worldwide. Of these, 79 have been arrested for sharing and distributing child sexual abuse material (CSAM).

Operation Stream is the largest operation ever handled by Europol experts in the fight against child sexual exploitation. It is also one of the biggest cases supported by Europol in recent years.

Catherine De Bolle, Europol Executive Director, commented: “The digital dimension has driven a rapid evolution in online child sexual exploitation, of-

fering offenders a borderless platform to contact and groom victims, as well as to create, store, and exchange child sexual abuse material. Some attempt to frame this as merely a technical or cyber issue – but it is not. There are real victims behind these crimes, and those victims are children.” As a society, we must act to protect our children.” (CR)

## Organised Crime

### EU-SOCTA 2025

**spot light** On 18 March 2025, Europol published its [EU Serious and Organised Crime Threat Assessment 2025](#) (EU-SOCTA 2025). The EU-SOCTA is Europol’s flagship report. Published every four years, it provides a comprehensive overview of the threats posed by serious and organised crime in Europe. The report identifies key criminal activities, the dynamics of criminal networks, and emerging trends. For the 2021 SOCTA Report [→eucrim 2/2021, 90](#).

In four chapters, the new report examines the changes in serious and organised crime, the tactics of serious and organised crime, the changing shape of the EU criminal landscape, and the geographies of criminal networks.

Overall, the report states that the profound changes taking place in serious and organised crime (SOC) are further exacerbating the threat they pose to the EU. The SOC threat is evident in a number of ways, such as:

- Double destabilising effect on the EU and its society (1) through the generation of illicit revenues and parallel economies, and (2) through criminal networks which increasingly act as proxies for hybrid threat actors (a form of cooperation that is mutually reinforcing);
- Being increasingly nurtured online, with more and very impactful criminal activities happening largely in the digital space;

- Accelerating by AI and other new technologies, making criminal operations more accessible and automated, increasing scale and reach of crime, and enhancing criminal capabilities.

In terms of crime areas, the EU-SOCTA 2025 identifies the following key threats:

- *Online threats* such as cyberattacks, online fraud schemes, (online) child sexual exploitation. Cyberattacks are increasingly state-aligned, targeting critical infrastructure and government structures. Online fraud schemes have become unprecedented in size, variety, sophistication, and reach and are expected to outpace other types of serious and organised crime. With generative AI being used to produce child sexual abuse material, (online) child sexual exploitation is transforming.

- *Physical threats* in cross-border crime areas like migrant smuggling, drug trafficking, firearms trafficking, and waste crime. All areas show a continuous diversification of *modi operandi*, shifting and further expanding under the influence of developments in technology, AI, and the online sphere.

The report concludes that the identified key threats have a number of elements in common that sustain and boost them in varying ways. Law enforcement must integrate these cross-cutting elements when designing approaches to fight the key criminal threats and it must confront reinforcing tactics, such as the use of digital platforms for money laundering activities, the infiltration of legal business structures, and the exploitation of young perpetrators. Developments need to be closely monitored – particularly in the EU neighbourhood but also beyond. (CR)

### New In-Depth Analysis on the European Ecstasy Market

On 27 March 2025, Europol and the European Union Drugs Agency (EUDA) published their latest [study on the Eu-](#)

[European market for MDMA](#) (ecstasy), covering aspects from production and trafficking to distribution and use. The report – a comprehensive threat assessment – also details the processes, materials, and criminal actors involved at different stages and levels of the market and defines recommendations for action at EU and Member State level.

According to the study, the EU is central to the global synthetic drugs landscape, with production in the EU serving both domestic and international markets. Around 12.3 million Europeans (aged 15–64) have used MDMA at least once in their lifetime, while an estimated 20 million people used MDMA worldwide in 2022. The European retail market for MDMA is estimated to be worth at least €594 million annually, corresponding to the consumption of around 72.4 million ecstasy tablets within the EU.

MDMA production is concentrated mainly in the Netherlands and Belgium. Dutch criminal networks play a significant role in the MDMA market, both within and outside the European Union. Europe's MDMA market has a global reach, supplying Oceania, Asia, and also Latin America.

In order to address the challenges associated with MDMA, the report identifies two key priorities:

- Improving intelligence on MDMA trafficking within Europe and to external markets;
- Reducing MDMA production and distribution.

Achieving these aims will require enhanced collaboration between EU Member States, international partners, and other key stakeholders, focusing on the exchange of operational and strategic information. In addition, increasing the availability of prevention, harm reduction, and treatment programmes will be essential to mitigate the harmful impact of MDMA on public health. In sum, the intelligence picture of the MDMA market must be enhanced. (CR)

### [Long-term JIT against Drug Traffickers Yields Significant Results](#)

For the past five years, the Norwegian and Danish authorities, with the support of Eurojust, have been operating a joint investigation team to combat drug trafficking. A recent [evaluation of this JIT](#) highlights the successful fight against an organised crime group (OCG) that was trafficking large quantities of different types of illicit drugs from Morocco to Denmark and Norway via Spain. As a result of the JIT that started in 2019:

- 83 suspects were sentenced to a total of 414 years' imprisonment in Norway;
- 69 perpetrators were sentenced to a total of 623 years' imprisonment in Denmark;
- More than 9600 kilos of cannabis, 675 kilos of cocaine, 355 kilos of amphetamines, 77 kilos of synthetic drugs, and 41 kilos of heroin were seized in the two countries, as well as various firearms;
- Other seized assets included several apartments and other properties, a vehicle, a boat, a motorbike, and luxury watches, as well as cash and cryptocurrencies, with an estimated total value of €15.6 million. (CR)

### [Trafficking in Human Beings](#)

#### [5th Progress Report on Fight Against THB](#)

Trafficking in human beings (THB) constitutes the second most widespread illicit economy in the world, reaching USD 20,000 profit per victim per annum, with the exploitation of victims in Europe and Central Asia being the most profitable. The risks for perpetrators remain low.

The European Commission's [fifth report on the progress made in the EU in combating Trafficking in Human Beings](#) (published on 20 January 2025) identifies key trends and main anti-trafficking actions from 2021 to 2024 and

provides an analysis of statistics for the period 2021–2022:

- 17,248 victims of trafficking were registered in the EU during the 2021–2022 reporting period, representing an increase of 20.5% compared to the 2019–2020 period. At the same time, the actual number of victims is likely to be significantly higher than the reported data suggests, as many victims remain undetected.
- 65% of all the victims in the EU were women and girls.
- While most of the victims of sexual exploitation were female (92%), men represent the majority of the victims trafficked for labour exploitation (70%).
- 46% of the registered victims in 2021–2022 were EU citizens and 54% were third country nationals, indicating a shift from previous years when the majority of registered victims were EU citizens (55%).
- The top-five EU citizenships of trafficked victims were Romanian, French, Hungarian, Bulgarian, and German.
- The top-five non-EU citizenships of trafficked victims were Nigerian, Ukrainian, Moroccan, Colombian, and Chinese.
- 34% of all victims were citizens of the country in which they were registered (internal trafficking).

Sexual exploitation remains the most common and labour exploitation the second most common form of trafficking in the EU. Forms of THB, other than sexual and labour exploitation, accounted for 14% of all victims. Such forms of exploitation include, for instance, forced criminal activities, forced begging, and illegal removal of organs.

- There was a 51% increase in victims of labour exploitation in 2021–2022 (5940), compared to the previous period (3940).
- Recruitment is carried out online with fraudulent job advertisements.
- High-risk sectors for labour exploitation include construction, agriculture, forestry, food processing, assembly

lines, hospitality, retail, carwashes, beauty and cleaning services, transportation and housekeeping. Newly emerging sectors are, for example, domestic care and nursing services, and parcel delivery. The football sector has emerged as a special area of exploitation in Portugal and Belgium.

Looking at child trafficking, the report states that children in the EU are trafficked for all forms of exploitation, mainly sexual exploitation, but also for forced criminality, forced begging, forced marriage, and labour exploitation. The decreasing trend of registered child victims in some Member States may be linked to the increase in online sexual exploitation, where many victims remain hidden.

To combat THB, the report examines the comprehensive approach taken under the EU Strategy on Combating Trafficking in Human Beings 2021–2025 ([→eucrim 2/2021, 92](#)). It outlines the following measures:

- The revision of Directive 2011/36/EU;
- The forthcoming launch of an Anti-trafficking Hub;
- The introduction of mandatory collection and sharing of statistics;
- National Strategies and Action Plans;
- Guidelines, protocols, and procedures;
- The new obligation for Member States to adopt and implement national Anti-trafficking Action Plans;
- The allocation of financial resources for combatting THB;
- The strengthened role of the EU Anti-Trafficking Coordinator;
- The mandatory establishment of national anti-trafficking coordinators.

The report emphasizes the need to reduce the demand for THB with various legislative measures, e.g., criminalising the knowing use of exploited services and addressing the responsibility of companies, including online platforms, to reduce demand and detect potential cases of THB. Further

key actions in combatting THB are partnerships with third countries and international organizations, law enforcement cooperation, (digital) and financial investigations, and operational actions to disrupt criminal networks engaged in THB and break their criminal business models.

Given that THB is closely linked with migrant smuggling, the report also underlines the need to address the legislative, operative, and funding measures related to the fight against migrant smuggling together with combating trafficking in human beings in the context of irregular migration. Ultimately, it calls for a victim-focused, gender- and child sensitive approach. While legislative measures have been taken, such as amendments to the Anti-Trafficking Directive or revision of the Victims' Rights Directive, non-legislative measures are also needed to achieve early identification, assistance, and protection of the victims. (CR)

#### Negative Impact Assessment for Anti-Smuggling Directive by EP Research Service

On 5 March 2025, the European Parliamentary Research Service ([EPRS](#)) [negatively evaluated](#) the Commission proposal for a revised directive laying down minimum rules to prevent and counter the facilitation of unauthorised entry, transit and stay in the Union ("Facilitation Directive"). The directive is intended to renew the existing regulatory framework for preventing the facilitation of unauthorised entry, transit and residence in the Union.

The proposal for a "Facilitation Directive" was part of a legislative package to counter migrant smuggling that was tabled on 28 November 2023 ([→eucrim 3/2023, 257–258](#)). The package also included a proposal for a Regulation to reinforce police cooperation and Europol's role in the fight against migrant smuggling and trafficking in human beings.

The EPRS study was conducted in view of supporting the European Parliament's position on the proposal. The competent LIBE Committee criticised that the Commission proposal lacked a thorough impact assessment, which should have included, for instance, the proposal's fundamental rights implications and compliance with relevant international legal standards.

In the "targeted substitute impact assessment", the EPRS critically reviewed the existing legal framework at EU level and its shortcomings in terms of transposition and implementation as well as the objectives of the Commission proposal. It also provides a legal analysis of the key provisions of the proposed directive and particularly scrutinizes their compatibility with the principles of legality and proportionality as well as the presumption of innocence.

According to the main findings of the EPRS, the proposed directive is not consistent with either international or EU standards, is also characterised by considerable uncertainties and sets out overly harsh penalties. Furthermore, human rights are insufficiently protected. The very broad scope of application carries the risk of not only covering actual (punishable) smuggling, but also individuals and organisations that provide humanitarian aid or legitimate services.

In light of the main findings and the main deficiencies detected in the Commission proposal, the EPRS study makes a series of recommendations. It remains to be seen to what extent the LIBE committee and the European Parliament will adopt the EPRS position. The [Council adopted its position](#) on the Commission proposal on 13 December 2024. (TW)

#### Lawyers Call for Changes to Anti-Smuggling Directive

In a [joint letter](#), several organisations of lawyers and organisations dealing with legal assistance, together with



various individual lawyers, called on EU legislators to adopt a narrow definition of the offence of “smuggling” in line with international standards and to include a mandatory and broad humanitarian exemption clause in the so-called “Facilitation Directive”. The draft Directive was tabled by the Commission on 28 November 2023 as part of a legislative package to counter migrant smuggling (→[eucrim 3/2023, 257–258](#)) and is currently negotiated by the Council and the European Parliament.

The signatories of the joint letter stress that the wide definition of the offence of “facilitation” risks criminalising legal humanitarian or family assistance to migrants. The Council’s general approach to introduce the material benefit component in the definition of “smuggling” is considered insufficient to avoid the criminalisation of solidarity or regular professional activities. In particular MEPs who work on the legislative dossier are urged to “to recognise the role of civil society in ensuring dignity, safeguarding fundamental rights of migrants and assisting Member States where their capacities are insufficient”. Only a narrow definition of the offence and a mandatory exemption can bring clarity and certainty.

Recently, also a study for the European Parliamentary Research Service negatively evaluated the Commission’s proposal for the “Facilitation Directive” (→[previous news item](#)). (TW)

## Procedural Law

### Procedural Safeguards

#### ECJ Ruled on the Rights of Vulnerable Persons in Criminal Proceedings

On 8 May 2025, the ECJ handed down a [ruling](#) on the scope of the rights of access to a lawyer and a vulner-

able person’s right to legal aid in line with Directive 2013/48 and Directive 2016/1919 ([Case C-530/23, Baraño](#)).

The referred questions were raised in respect of the treatment of a defendant in Poland who was charged with “driving a car under the influence of a drug having a similar effect to alcohol” and who suffered from psychotic mental health condition during the investigative phase of the criminal proceedings.

The ECJ clarified that, in line with Directives 2013/48 and 2016/1919, the EU Member States have the following obligations:

- To ensure that the vulnerability of an accused person or of a suspect is ascertained and acknowledged before that person or suspect is questioned in the context of criminal proceedings or before specific investigative or evidence-gathering measures have been carried out in relation to that person or suspect;
- To ensure that such persons or suspects have access to a lawyer under legal aid for the purposes of those proceedings without undue delay and, at the latest, before questioning by the police or by another law enforcement authority or by a judicial authority, or before the investigative or evidence-gathering act in respect of which that person or suspect is required or permitted to attend is carried out;
- To reason decisions concerning, first, the assessment of the potential vulnerability of a suspect or an accused person and, second, the refusal to grant legal aid to a vulnerable person and the choice to question that person in the absence of the lawyer; these decisions must be the subject of an effective remedy.

By contrast to the [Advocate General’s opinion](#), the ECJ held, however, that the EU Directives do not preclude national legislation which, in criminal proceedings, do not allow for a court to declare inadmissible incriminat-

ing evidence contained in statements made by a vulnerable person during questioning by the police, by another law enforcement authority or by a judicial authority in breach of the rights laid down by Directive 2013/48 or 2016/1919. But this is under the condition that, in criminal proceedings, the adjudicating court is in a position, first, to verify that those rights, read in the light of Art. 47 and Art. 48(2) of the EU Charter of Fundamental Rights, have been respected and, second, to draw all the inferences from that breach, in particular as regards the probative value of the evidence obtained in those circumstances. (TW)

#### GC Strengthened Procedural Rights in Disciplinary Proceedings against MEP

On 12 March 2025, the General Court [ruled](#) in Case [T-349/23](#) (*Semedo v Parliament*) on the requirements for a fair trial in disciplinary proceedings within the European Parliament (EP).

In March 2022, the EP’s Advisory Committee launched an investigation into former MEP *Monica Semedo*. The proceedings were initiated following a complaint of psychological harassment by her former parliamentary assistant. In November 2022, the committee concluded that her conduct constituted psychological harassment and recommended that her daily allowance be suspended for 20 days. One month later, Ms Semedo received an anonymised version of the investigation report with an invitation to comment. However, her request to inspect the full file in January 2023 was rejected. In the following April, the EP’s President, *David Sassoli*, found that certain conduct on the part of Ms Semedo constituted psychological harassment and imposed a reduced penalty in the form of forfeiture of entitlement to the subsistence allowance for a period of 10 days. Monica Semedo then brought an action for annulment before the EU’s General Court (GC).



The Court found that the decisions of the EP's President were void due to substantial procedural errors with regard to Ms Semedo's defence rights and must therefore be annulled. In particular, the applicant was denied access to a summary of the witness statements and to essential documents on which the allegations against her were based. However, these documents played a decisive role in establishing the harassment and imposing the penalty. This deprived the person concerned of the opportunity to defend herself adequately, which inevitably affected the content of the contested decisions. (TW)

## Data Protection

### Council Concluded EU-Canada PNR Agreement

On 14 April 2025, the [Council of the European Union concluded](#), on behalf of the Union, the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (PNR) data. The [European Parliament gave its consent](#) to the deal on 12 March 2025. As a result, the EU formally completed its internal procedures for the ratification of the Agreement. In order to become binding for both parties, the Agreement still needs to be ratified by Canada.

The Agreement provides for the transfer of passenger name record data from the EU to Canada for the purposes of preventing, detecting, investigating and prosecuting serious crime and terrorism. It was signed in October 2024 ([→eucrim 3/2024, 191](#)). Negotiations for a new EU-Canada PNR deal became necessary after the CJEU had found in 2017 that a previous agreement on PNR transfers to Canada was incompatible with fundamental rights protection in the EU ([→eucrim 3/2017, 114–115](#)). (TW)

### ECJ: Overall Turnover of Entire Company Group Decisive for Fine Calculation if GDPR Was Infringed

According to the [ECJ's judgment of 13 February 2025 in Case C-383/23 \(ILVA\)](#), a fine for a violation of the General Data Protection Regulation (GDPR) may be calculated on the basis of the global turnover of an entire group of companies.

#### ► Background of the case

The case, referred for a preliminary ruling by the High Court of Western Denmark (*Vestre Landsret*), clarified how fines under Art. 83(4) to (6) GDPR should be calculated for a company that is part of a corporate group. In the underlying proceedings in Denmark, ILVA A/S, a furniture retailer and subsidiary of the Lars Larsen Group, had been charged with failing to comply with GDPR obligations concerning the retention of personal data of former customers.

The Danish prosecutor was seeking a fine, partly based on the overall turnover of the corporate group and arguing that the concept of an "undertaking" in Art. 83(4)–(6) GDPR should align with the competition law understanding in Arts. 101 and 102 TFEU. The District Court of Aarhus disagreed, finding ILVA liable only for its own actions and imposing a lower fine calculated on its own turnover. The case was subsequently appealed.

#### ► ECJ ruling

The ECJ held that the term "undertaking" in Art. 83 GDPR must indeed be understood in the same way as it is in EU competition law. This interpretation entails that a corporate group may be treated as a single economic unit when one of its entities commits an infringement. Consequently, for purposes of determining the *maximum amount* of the fine, the supervisory authority or national court may take into consideration the entire worldwide turnover of the entire economic entity (i.e., the group), not just the subsidiary's turnover.

The Court emphasized, however, that the actual *amount* of the fine must be effective, proportionate, and dissuasive in each individual case, taking into account the specific circumstances listed in Art. 83(2) GDPR, such as the nature and gravity of the infringement and the controller's responsibility. It also noted that, even when fines are imposed by criminal courts (as in Denmark, where GDPR fines are considered criminal penalties), and not handled as administrative sanctions, there are no obstacles of principle since criminal courts must at all times respect the rules applicable in criminal matters and ensure the principle of proportionality when calculating the fines.

#### ► Put in focus

In sum, the ECJ confirmed that the GDPR's concept of an "undertaking" incorporates the competition law notion of a single economic unit. Accordingly, when calculating GDPR fines for group-affiliated entities, the turnover of the entire group may be considered – in this way ensuring that fines are not only proportionate to the infringement but also to the economic capacity of the offender.

The ruling could set a precedent for other digital laws, as the Digital Markets Act, the Digital Services Act and the AI Act, for example, provide for similar sanction mechanisms. (AP)

## Ne bis in idem

### ECJ: Double Penalties for an Energy Company May be Justified

**spot light** On 30 January 2025, the ECJ ruled on the limitation of the *ne bis in idem* principle (Art. 50 of the Charter of Fundamental Rights of the European Union [CFR]) in case of two fines imposed on an economic operator in administrative proceedings. The [ruling](#) consolidates the ECJ's case law on the interpretation of Art. 50 CFR for ad-

ministrative punitive proceedings. The case is referred to as [Case C-205/23, Engie România](#).

#### ► *Facts and background of the case*

The case at issue results from a Romanian natural gas supplier, Engie România SA, which was subject to two administrative penalties for identical facts: On the basis of the Romanian laws transposing Directive 2009/73 concerning common rules for the internal market in natural gas, the Romanian Energy Sector Regulatory Authority imposed a fine of RON 800,000 (€160,000) to the company for breach of transparency rules. On the basis of the Romanian laws transposing Directive 2005/29 concerning unfair business-to-consumer commercial practices in the internal market, the Romanian Consumer Protection Authority imposed a fine of RON 150,000 (€30,000) for “misleading and aggressive commercial practice with regard to consumers”. Both fines have been based on the company’s conduct of obscure adjustments of prices for the supply of natural gas to its customers. The referring court, the Tribunalul București (Regional Court, Bucharest, Romania), wondered in essence whether the duplication of the “penalties” were in line with Art. 50 CFR, read in conjunction with Art. 52(1) CFR.

#### ► *The ECJ’s reasoning*

The ECJ first recalled that the two administrative fines imposed can be regarded as “criminal penalties”, as required by Art. 50 CFR, if – regardless of the classification in national law – there is account of the intrinsic nature of the offence or the degree of severity of the penalty which the person concerned is liable to incur. The degree of severity must be assessed by reference to the maximum penalty for which the relevant provisions provide. The criterion regarding the intrinsic nature of the offence, involves ascertaining whether the penalty at issue has, *inter alia*, a punitive purpose, without regard to

the fact that it also pursues a deterrent purpose. By contrast, measures which merely repair the damage caused by the offence at issue are not criminal in nature. The ECJ here refers to its previous judgments in *bpost* ([→eucrim 2/2022, 116–118](#)) and *Volkswagen Group Italia* ([→eucrim 2/2023, 155–156](#)). Whether the requirements are fulfilled in the present case is for the referring court to ascertain.

In the affirmative, the ECJ reiterated its case law that the protection from double penalties under Art. 50 CFR is limited: Duplication of criminal proceedings or penalties can be justified on the basis of Art. 52(1) CFR. This is the case if the following conditions are met:

- There are clear and precise rules making it possible to predict which acts or omissions may be subject to a duplication of proceedings and penalties, and to ensure coordination between the two competent authorities;
- The two sets of proceedings concerned have been conducted in a sufficiently coordinated manner and within a proximate timeframe; and
- All the penalties imposed correspond to the seriousness of the offences.

Also this is finally up to the referring court to determine. However, the judges in Luxembourg indicated that, according to the case file, there has been a close connection in time between the two sets of administrative (punitive) proceedings at issue, both proceedings pursued different objectives (compliance with energy sector rules vs consumer protection), and there has been cooperation and exchanges of information between the two Romanian authorities. Thus, it is likely that the duplication of the two administrative proceedings leading to two fines against Engie Romania can be justified.

#### ► *Put in focus*

The judgment in *Engie România* essentially reiterates the ECJ’s previous

case law on the culmination of two or more administrative penalty proceedings. Firstly, the scope of protection of the European *ne bis in idem* principle in Art. 50 of the Charter must be interpreted broadly. If a sanction has a punitive – not necessarily deterrent – purpose, fines imposed by administrative/regulatory authorities must also be regarded as “criminal penalties”.

Secondly, the ECJ confirms that, provided that different legal interests are being pursued and there is sufficient coordination between the authorities involved, an economic operator must expect to be sanctioned more than once for the same misconduct. The criteria established by the ECJ for permissible double punishment are not very strict. Thus, there may be often green light for the imposition of double sanctions. Companies must adapt to this and adjust their compliance strategies accordingly. (TW) ■

## Victim Protection

### ECJ Ordered Several Member States to Financial Penalties for Failing to Transpose Whistleblowers Directive

In [rulings handed down on 6 March 2025](#), the ECJ sanctioned five EU Member States for having transposed the Whistleblowers Directive too late or not yet at all.

[Directive \(EU\) 2019/1937](#) of the European Parliament and of the Council of 23 October 2019 “on the protection of persons who report breaches of Union law” (Whistleblowers Directive) establishes rules and procedures to protect whistleblowers, individuals who report information they acquired in a work-related context on breaches of EU law in key policy areas. Breaches include both unlawful acts or omissions and abusive practices. According to the Directive, whistleblowers can choose whether to report first internally or to directly report externally to the competent authorities. The Directive

obliges Member States to provide several protection and support measures to whistleblowers ([→eucrim 4/2019, 238–239](#)). The Directive had to be transposed by 17 December 2021.

Among the countries which transposed the Whistleblower Directive far too late is Germany. The Federal Republic, among other things, justified the delay by pointing out that it had to conduct complex technical and political discussions as regards the extension of the material scope beyond the one determined by the Directive in order to offer a high level of protection to whistleblowers. It also argued that the legislative process had been interrupted due to the parliamentary elections in 2021 and that the conciliation committee had to be called upon during the legislative process. However, these arguments did not succeed before the ECJ. The ECJ referred to its settled case-law: a Member State cannot plead provisions, practices or situations prevailing in its domestic legal order to justify failure to observe obligations arising under EU law such as failure to transpose a directive within the period prescribed. The ECJ ruled that Germany has to pay a lump sum of €34 million as a financial penalty for its late implementation of the Whistleblowers Directive.

The ECJ has also sanctioned Luxembourg, Hungary, the Czech Republic and Estonia for failure to transpose the Whistleblowers Directive. The Czech Republic must pay a lump sum of €2.3 million, Hungary a lump sum of €1.75 million, and Luxembourg a lump sum of €375,000. Estonia has to pay a lump sum of €500,000 plus a daily penalty of €1,500 since the failure to comply has persisted.

The EU Commission brought infringement proceedings before the ECJ against several Member States for not having transposed the Whistleblowers Directive in 2023. In its [judgment of 25 April 2024](#), the ECJ already imposed sanctions on Poland for fail-

ing to implement the Whistleblowers Directive. (TW)

## Freezing of Assets / Confiscation

### Project A.S.S.E.T Results in Largest-Ever Operation to Seize Criminal Assets

From 13 to 17 January 2025, Europol brought together more than 80 financial experts from around the world, including from the private sector, together with 43 law enforcement agencies from 28 countries and Interpol, to carry out the largest ever operation to seize criminal assets: [Project A.S.S.E.T](#) (Asset Search & Seize Enforcement Taskforce). During the days of the operation, the specialists' knowledge and expertise was pooled in order to establish a new organisational workstream to identify, freeze, and seize criminal assets using all available means. As a result, the project identified the following assets:

- 53 properties, eight of which were valued at €38.5 million;
- Over 220 bank accounts, including one with a balance of US\$5.6 million;
- 15 companies, over 20 yachts and luxury vehicles, four of which were valued at over €600,000;
- 83 cryptocurrency addresses and wallets;
- The freezing of €200,000 in cryptocurrencies.

In addition, further investigations resulting from the action days led to the seizure of €27 million in cryptocurrency alone.

Project A.S.S.E.T is an important milestone for Europol's focus on combating all forms of serious international and organised crime by bringing relevant partners together. In this regard, a crucial element of Project A.S.S.E.T. was the participation of financial actors from the private sector, especially organisations from the banking sector and cryptocurrency exchanges. Public-private partnerships

between Europol and the financial sector is a priority for the law enforcement agency. In this context, see also the conclusions/recommendations of the PartFin project [→B. Vogel and M. Lassalle, "Developing Public-Private Information Sharing to Strengthen the Fight Against Money Laundering and Terrorism Financing", eucrim 4/2023, 384–392](#). (CR)

## Cooperation

### Police Cooperation

#### Civil Rights Organisations Criticise Predictive Policing Projects

In April 2025, civil liberties, human rights and justice organisations and experts voiced their concerns over the development of the use of predictive policing systems by national police forces and the concerning development of AI-supported automated police decision-making systems.

On 15 April 2025, civil rights organisations *Statewatch*, the *Ligue des droits humains* and the *Liga voor mensenrechten*, jointly published a [report on "predictive" policing and data-profiling in Belgium](#). The report examined and analysed "predictive" policing initiatives and ambitious digitalisation projects in the Belgian police. These included:

- Location-focused "predictive" policing systems used by local Belgian police forces;
- The databases that are or will be used to inform those systems;
- The Belgian Federal Police "i-Police" project, designed to use data from police and other public agencies, as well as a range of other data sources, to inform police decision-making and activities.

The report highlights several serious problems in the context of the use of advanced data analysis techniques to try to "predict" crime:

- Lack of transparency at both the local and federal levels and limited information available;
- Significant shortcomings in managing and controlling databases by the Belgian police forces;
- Often biased or unfounded information in the databases;
- Predictive policing systems produce structural inequalities and discrimination against the most marginalised groups in society.

In conclusion, the report says: “[I]t is imperative that Belgium prohibits the use of ‘predictive’ policing and automated decision-making systems in policing and criminal justice settings. By banning these systems, Belgium can take a significant step towards building a more equitable, just, and democratic society. It is an opportunity to reaffirm the commitment to upholding fundamental rights, promoting equality, and maintaining the principles of justice and accountability.”

On 9 April 2025, Statewatch criticised the [United Kingdom’s system for “predicting” the re-offendering risk of offenders or alleged offenders](#). According to the UK Ministry of Justice, the system uses a combination of “structured professional judgement” and risk prediction algorithms to generate “risk scores.” The manual assessment, usually conducted by the Prison Offender Manager (POM, a Prison Service official), gathers information on various categories. Statewatch stressed that over 1,300 people are profiled daily by this AI system. Statewatch criticised that despite serious concerns over racism and data inaccuracies, the system continues to heavily influence decision-making on imprisonment and parole. New digital tools are on the way to replace the system in 2026. In addition, the UK government is working on other [predictive policing projects](#) as well as on a [bill](#) that would allow police decisions to be made solely by computers, Statewatch said. (TW)

## Judicial Cooperation

### ECJ: Surrender to UK Can Be Done Despite Hardening of Conditions for Release

On 3 April 2025, the ECJ ruled in [Case C-743/24 \(\*Alchaster II\*\)](#) that a hardening of the conditions for release on licence from custody against a requested person does not, in principle, preclude surrender of that person from an EU country to the UK.

#### ► Background of the case

In its judgment *Alchaster I* of 29 July 2024 ([→eucrim 2/2024, 137–138](#)), the ECJ, at the request of the Irish Supreme Court, clarified the conditions under which arrest warrants issued by the United Kingdom can be executed in the EU. In particular, the ECJ defined the limits under which violations of fundamental rights in the United Kingdom can lead to the refusal of extradition under the Trade and Cooperation Agreement (TCA) between the European Union and the United Kingdom. The Irish Supreme Court has again referred the matter to the ECJ for a preliminary ruling in the same surrender proceedings. It now wishes to know, in a specific application of the fundamental rights test established by the Luxembourg Court in *Alchaster I*, whether the term “heavier penalty” enshrined in Art. 49(1), second sentence CFR also covers cases in which the rules on release on licence have changed.

In the main proceedings, a person is sought for terrorism-related offences by authorities in Northern Ireland. In the extradition proceedings in Ireland, the requested person argued, in particular, that Northern Ireland changed the licence regime for sentences of imprisonment to his detriment: On the date of the alleged commission of the offences at issue (July 2020), he could automatically have been eligible for release on licence after having served half of that sentence. As from 30 April 2021, under amended rules, he has a right to release on licence only if he

has served at least two thirds of such sentence and under the condition that an assessment of dangerousness by a specialised authority is negative. He claims that this amendment infringes the principle that offences and penalties must be defined by law as provided for in Art. 49(1) CFR. The Irish Supreme Court wondered whether this is really the case here so that surrender may be denied by Ireland due to the UK risking an infringement of this fundamental Charter right.

#### ► The ECJ’s judgment

Referring to the case law of the European Court of Human Rights on Art. 7 ECHR, [the judges in Luxembourg state](#) that the fact that changes to the licence regime lead to a hardening of the detention situation does not necessarily have to be regarded as entailing the imposition of a heavier penalty, within the meaning of the second sentence of Art. 49(1) CFR.

The ECJ explains this finding as follows: “[I]t stems from the separation between the concept of ‘penalty’, understood as being the sentence handed down or capable of being handed down, on the one hand, and that of measures relating to the ‘execution’ or ‘enforcement’ of the penalty, on the other. It applies not only to the extension of the eligibility threshold for release on licence, but also to changes to other conditions to which the grant of a release on licence is subject or to the procedural rules governing such a grant. Thus, in so far as those changes do not, in essence, repeal the possibility of such release and do not lead to an increase in the intrinsic seriousness of the penalty provided for on the date of the alleged commission of the offences at issue, their application to offences committed before their entry into force does not infringe the second sentence of Article 49(1) of the Charter.”

According to the ECJ, a convicted person preserves the possibility for release on licence also with the new



regime. The extension of the period of possible release also leaves unchanged the maximum period in which the person concerned can be placed in custody. Furthermore, the application of a criterion based on the danger posed by the sentenced person at the time of his or her possible release on licence is, by its nature, linked to the execution of the penalty.

In sum, there should be no obstacle for surrender of the requested person. (TW)

### European Arrest Warrant

#### ECJ: VAT Fraudster Must Be Surrendered to Spain

On 10 April 2025, the ECJ ruled in [Case C-481/23 \(Sangas\)](#) that the execution of a European arrest warrant (EAW) cannot be refused if it is intended solely to ensure that the requested person is present at resumed criminal proceedings in the issuing State, nor if there is no jurisdiction for the acts constituting the offence under the criminal law of the executing State.

In the main proceedings, the Audiencia Nacional (National High Court, Spain) is challenging the non-execution by the Romanian courts of an EAW issued against JMTB. In 2022, the Audiencia Nacional sentenced JMTB, a Spanish national residing in Romania, to a number of prison terms and heavy fines as co-perpetrator of a huge value added tax (VAT) fraud on the sale of hydrocarbons. The accused lodged an appeal on point of law but, at the same time, fled to Romania, his country of residence. The Spanish court issued an EAW and sought surrender to Spain in order to be present in the appeal proceedings. However, the Curtea de Apel Alba Iulia (Court of Appeal, Alba Iulia, Romania) refused execution of the EAW arguing that, first, the accused was residing in Romania and, secondly, criminal proceedings were statute-barred un-

### Transfer of Sentenced Persons

#### *Italian Supreme Court Applies Manifest Error Doctrine: Personal Drug Use Cannot Be Treated as Illicit Trafficking under EU Mutual Recognition Framework*

On 14 March 2025, in a landmark ruling, the Italian Court of Cassation clarified the powers of the executing state's obligations under Framework Decision 2008/909/JHA concerning the mutual recognition of criminal judgments imposing custodial sentences (Corte di Cassazione, sez. VI penale, sentenza n. 10395/2025). An unofficial machine translation of the ruling into English is available at the [website of canestriniLex](#).

The case involved the recognition in Italy of two German convictions for possession of narcotics for personal use, submitted with a certificate ticking the box for "illicit trafficking in narcotic drugs and psychotropic substances" – a category exempt from the double criminality check under said Framework Decision. In overruling the lower courts' decision to recognize the German convictions, the Italian highest court ruled that while the executing authority is in principle bound by the classification made by the issuing state (cf. CJEU, Case C-136/20, LU), it may contest a "manifest error" in the completion of the certificate. The Court of Cassation relied on Framework Decision 2004/757/JHA, which provides minimum rules for drug offenses. Article 2 of this Framework Decision excludes any conduct committed solely for personal consumption, as defined by national laws from "illicit trafficking".

In case at issue, classifying the simple possession for personal use, which is not a crime under Italian criminal law, as illicit drug trafficking constituted such a "manifest error", according to the Court of Cassation. It ruled that possession for personal use, although criminalized in some EU Member States, falls outside the EU-harmonized concept of trafficking and does not correspond to an Italian offense under Article 73 of the Italian Drug Bill, DPR 309/1990, when not linked to distribution.

The judgment emphasizes the mandatory interlocutory procedure under Article 10(3) of Legislative Decree 161/2010 for partial recognition, requiring the Italian court to consult with the German authorities before proceeding. (Nicola Canestrini)

der Romanian law. The Audiencia Nacional referred the case to the ECJ asking, in essence, whether the Romanian appeal court could invoke the optional refusal grounds of Art. 4(6) and Art. 4(4) of [Framework Decision 2002/584/JHA](#) on the European arrest warrant (FD EAW).

The [ECJ replied](#) that the Spanish EAW at issue was adopted not "for the purposes of execution of a custodial sentence or detention order", within the meaning of Art. 4(6) FD EAW, but for the purposes of the other situation envisaged in Art. 1(1) FD EAW, namely that of criminal prosecution. Thus, there is no ground for refusing surrender solely on the basis of the requested person's residence.

With regard to the argument of statute limitations, the ECJ recalled that Art. 4(4) FD EAW permits the executing judicial authority to refuse to execute an EAW where the criminal prosecution of the requested person is statute-barred according to the law of the executing Member State and the acts fall within the jurisdiction of that State under its own criminal law. This wording means that the two conditions of Art. 4(4) FD EAW must be met cumulatively. It is, however, apparent in the case at issue that all the acts had been committed in Spain and constituted tax evasion offences affecting the economic interests of that Member State, so that Romania lacks jurisdiction. (TW)



## Law Enforcement Cooperation

### Third Phase of SIRIUS Project Launched

In January 2025, Europol and Eurojust launched the [third phase of the SIRIUS project](#), an initiative to support national law enforcement agencies (LEAs) and judicial authorities (JAs) in the field of electronic evidence (for the last SIRIUS Report → [eucrim 4/2024, 293–294](#)).

New EU-wide legislation (such as the EU Electronic Evidence legislative package → [eucrim 2/2023, 165–168](#)), together with key international agreements (such as the Second Additional Protocol to the Budapest Convention (→ [eucrim 2/2022, 128](#)) and the agreed draft text for a UN Convention on Cybercrime), are reshaping the legal and operational landscape surrounding electronic evidence. Therefore, Phase 3 of the SIRIUS project will continue to support LEAs, JAs, and service providers in navigating the increasingly complex legal framework by providing a range of services such as guidance, training, and tools to help access data held by service providers.

Over the next several years, project activities will include the development of investigative tools, the organisation of high-impact events, and expanded capacity building to meet the urgent needs of LEAs and JAs. Geographically, the third phase of the SIRIUS project aims to strengthen cooperation between EU and non-EU countries that are of particular importance for the implementation of the new legislation. (CR)

### Ethical Decision-Making When Assessing Technologies in Law Enforcement

On 20 February 2025, Europol published a new report providing law enforcement agencies with a structured approach to evaluating new technologies while upholding fundamental rights and public trust. The report titled [Assessing Technologies in Law En-](#)

[forcement: A Method for Ethical Decision-Making](#) is intended to be a living, dynamic document that will serve as a permanent resource for law enforcement and policy makers.

The first part of the report describes a method for applying ethics and core values to practical decision-making: a seven-step ethical assessment method to help law enforcement agencies meet the challenges of digital transformation. It aims to ensure that the adoption and use of new technologies are consistent with core values such as transparency, fairness, privacy, and accountability. The seven steps to be used in evaluating technology are:

- (1) Description of the moral problem;
- (2) Collection of relevant facts about the case, such as facts about the technology and information about the context and relevant legislation;
- (3) Mapping of the different perspectives of the parties affected by the technology;
- (4) Explanation and identification of

the most important normative values relevant to the case, such as transparency, fairness, privacy, and accountability but also honesty, autonomy, beneficence, non-maleficence, social justice, etc.;

- (5) Formulation of value-based solutions, identification of the options;
- (6) Further scrutiny of the value-based options identified in the fifth step by considering their correctness and consequences; consequences for permissible options;
- (7) Summary of the process to ensure coherence/consistency of reasoning and choice.

In the second part of the report, cases of use are outlined to illustrate the method. Examples include video analytics technology, measuring the risks of reoffending in cases of gender-based violence, model analysis of open-source data scraping, using a chatbot to prevent child sexual abuse online, and automated analysis of large and complex datasets. (CR)



## Council of Europe

*Reported by Thomas Wahl*

## Foundations

### Rule of Law

#### CoE Convention on Protection of Lawyers Opened for Signature

On 13 May 2025, the new [Council of Europe Convention for the Protection of](#)

[Profession of Lawyer](#) was opened for signature. The first signatories include 17 Council of Europe member states.

The Convention for the Protection of Lawyer is the first-ever international treaty that aims at ensuring better protection of the profession of lawyer and hence responding to the rising trend of attacks, threats, harassment and

intimidation on account of, as well as improper hindrance and interference in their professional activities. The Convention obliges the parties to take measures in order to ensure the right to practise the lawyer profession with independence and without discrimination, to avoid improper hindrance and interference and to ensure protection from attacks, threats, harassment and intimidation.

The Convention applies to the professional activities of lawyers and of their professional associations. It is also applicable to (1) persons who have either been refused the qualification of lawyer or a licence to practise or has had these revoked or suspended; and (2) persons who are recognised by an international court or tribunal, or a body established by an international organisation, as competent to act in proceedings before it when advising on or acting in such proceedings.

The substantial part of the Convention's provisions relate to the following:

- Obligations towards the functioning of professional lawyer associations, which must be independent, self-governing bodies;
- Obligations regarding the entitlement to practise;
- Obligations to ensure the professional rights of lawyers;
- Obligations to ensure the freedom of expression of lawyers;
- Obligations towards disciplinary actions and proceedings against lawyers;
- Protective measures vis-à-vis individual lawyers and professional associations.

The Convention provides for a specific monitoring mechanism. Compliance will be ensured by "the Group of Experts on the Protection of the Profession of Lawyer" (GRAVO) and a Committee of the Parties.

Accession to the Convention is also permitted for non-Council of Europe member states. In order to enter into force, the Convention must be ratified

by at least eight countries, of which six must be member states of the Council of Europe.

*Eucrim* will regularly report on the status of signatures and ratifications in its section "Documentation → [CoE Ratifications](#)" (CETS 226).

## European Court of Human Rights

### 2024 Annual Report on Execution of ECtHR Judgments

On 19 March 2025, the Committee of Ministers of the Council of Europe published its [annual report](#) on the supervision of the execution of judgments and decisions of the ECtHR in 2024. The report includes country-by-country information on new cases, pending cases and cases closed for all 46 Council of Europe member states as well as an overview of the main trends and challenges and the Committee's Department for the Execution of ECtHR Judgments (DEJ) activities in cooperation, assistance and dialogue during the year.

The Committee of Ministers stressed that 2024 was a year with special significance, as the Council of Europe celebrated its 75th anniversary. One of the key achievements in the three-quarters of a century since its founding is the extraordinary contribution of the system established by the European Convention on Human Rights to the protection and promotion of human rights and the rule of law in Europe, as well as its central role in the maintenance and promotion of democratic security and peace throughout the continent. According to the report, this is needed now more than ever.

The report highlights that Ukraine continued to actively engage in the implementation of ECtHR judgments in 2024 (resulting in the closure of 75 cases) despite considerable challenges caused by Russia's on-going war of aggression. The key figures of the 2024 annual report include:

- 992 cases were transferred from the ECtHR to the Committee of Ministers for supervision;
- 194 of the 992 cases were "leading" cases that regularly require action to be taken by the CoE member states to prevent the same violations happening again;
- 798 of the 992 cases were repetitive cases, based on known problems that had already been identified by the Court;
- A total of 894 cases were closed by the Committee of Ministers during 2024, including 161 leading cases and 733 repetitive cases;
- At the end of 2024, a total of 3,916 cases were pending full implementation, including 1,149 leading cases and 2,767 repetitive cases.

The Committee of Ministers also reported on the implementation of the 2023 [Reykjavik Declaration](#) in which the heads of state and government of the CoE member states recommitted to resolving the systemic and structural human rights problems identified by the ECtHR and underlined the fundamental importance of the full, effective and prompt execution of the Court's judgments and the effective supervision of that process to ensure the long-term sustainability, integrity and credibility of the Convention system. They also emphasised the need for a co-operative and inclusive approach, based on dialogue, in the supervision process to assist states and overcome the challenges and obstacles encountered.

### Further Language Versions of ECtHR's Knowledge Sharing Platform

On 13 March 2025, the ECtHR [launched](#) Romanian, Turkish and Ukrainian language versions of its [Knowledge Sharing platform](#) (ECHR-KS). The platform is a tool for disseminating knowledge of ECtHR case-law and widening understanding of the Court's jurisprudence among the public. Users can get information on the case-law on each article of the Convention and its Protocols

as well as on transversal themes, such as data protection, prisoners' rights, and terrorism. The platform complements the ECtHR's comprehensive database HUDOC.

## Specific Areas of Crime

### Corruption

#### Denmark Blamed for Non-Implementation of GRECO Recommendations

On 7 April 2025, a high-level delegation of [GRECO urged Danish officials](#) to take measures in order to implement recommendations from GRECO's fourth and fifth round evaluation reports. GRECO particularly called on Denmark to fully implement GRECO's recommendations to prevent corruption and strengthen integrity within the Parliament, the central government (persons with top executive functions) and the police force.

GRECO noted that almost 6 years after the adoption of its 2019 fifth round evaluation report on Denmark ([→eucrim 3/2019, 184](#)), only 2 out of 14 recommendations have been implemented in full. Moreover, 11 years after the adoption of the 2014 fourth round evaluation report ([→eucrim 2/2018, 58](#)), only 2 out of 6 recommendations have been fully implemented. This raises concerns about Denmark's frameworks to effectively prevent corruption in the public sector. Outstanding recommendations include for instance:

- Developing a strategy for the integrity of persons with top executive functions on the basis of risk analysis;
- Adopting a code of conduct for persons with top executive functions, including practical guidance, and introducing a mechanism of supervision and enforcement;
- Improving public access to information;

- Developing a streamlined system for authorisation and follow-up of secondary activities within the police.

At the end of March 2025, GRECO published [two reports detailing the deficiencies](#) of Denmark to implement the recommendations of the 2014 and 2019 GRECO reports.

### Money Laundering

#### MONEYVAL: Fifth Round Evaluation Report on Guernsey

On 10 February 2025, MONEYVAL published its [5th round mutual evaluation report on Guernsey](#), a self-governing dependency of the British Crown. The report acknowledged Guernsey's good understanding of the risks of money laundering/terrorist financing (ML/TF) and its highly effective application of targeted financial sanctions. Positively assessed is also the high-quality of analytical reports and strategic analysis by Guernsey's Financial Intelligence Unit (FIU). However, these products are used by law enforcement authorities to initiate investigations only to a limited extent. The quality of suspicious activity reports (SARs) remains a concern, in particular those from the e-gambling sector generally have limited intelligence value. Other key findings of MONEYVAL's report include the following:

- The types of ML investigated and prosecuted in the assessment period have only to some extent been in line with the risk profile of the Bailiwick, mainly due to the previous, less risk-based approach of the authorities;
- In addition, despite the country's risk profile, no legal persons have been investigated or prosecuted for ML in the assessment period and most cases related to low-level ML conduct;
- Proceedings for conviction-based confiscation as well as civil forfeiture have been routinely launched as result of financial investigations pursued alongside investigations into ML and

predicate crimes, even though their results remained moderate;

- Understanding of the specific ML risks in the material sectors is generally good and business and customer risk assessments are regularly conducted/updated; there is, however, room for improvement, e.g. better mitigating risk measures associated with complex corporate structures in the sectors of trust and company service providers as well as investment;

■ Regulatory authorities, such as the Guernsey Financial Services Commission (GFSC) and the Alderney Gambling Control Commission (AGCC) have a very good understanding of risks; however, also here, there is room for improvement, e.g. with regards to risk data for trust and company service providers and risk categorisation;

- The GFSC and AGCC exercise their enforcement powers, however there are shortcomings in effectively sanctioning entities;

■ Guernsey has comprehensive measures to prevent the misuse of legal persons and arrangements for ML/TF, and to ensure beneficial ownership transparency for legal persons; registries perform effective checks at registration and upon changes to ensure data accuracy;

- Law enforcement authorities seek and provide international cooperation through various formal and informal channels, but these possibilities appear to be not fully exhausted (such as the use of CARIN network by the Economic and Financial Crime Bureau);

■ The Guernsey FIU cooperates regularly and effectively with its foreign counterparts (mainly the UK) actively seeking and providing information in a timely way and good quality; however, the number of requests to foreign counterparts appears not to be in line with the country's risk profile as an international financial centre.

Guernsey is expected to report back about the measures taken on MONEYVAL's recommendation by May 2027

under MONEYVAL's regular follow-up reporting process.

## Counterfeiting & Piracy

### First Monitoring Report of MEDICRIME Convention

**spot light** On 2 April 2025, the [first monitoring report](#) on the implementation of the Council of Europe Convention on the Counterfeiting of Medical Products and Similar Crimes Involving Threats to Public Health (MEDICRIME Convention) was released. The MEDICRIME Convention is the first binding international instrument in the criminal law field on the counterfeiting of medical products and similar crimes; it entered into force on 1 January 2016 ([→eucrim 2/2016, 84–85](#)).

The first monitoring round of the implementation of the MEDICRIME Convention has focused on the protection of public health through the MEDICRIME Convention in times of pandemics, including the COVID-19 crisis. The report covers this theme in 13 of the 23 States which were Parties to the Convention at the time the monitoring round report was adopted. The monitoring round collected information and identified measures taken in eight areas:

- Prevention and training;
- Education of civil society on good practices;
- Protection of victims' rights;
- Cooperation and exchange of information between authorities/bodies;
- Detection of counterfeit medical products;
- Investigation and prosecution of offenders for intentional crimes related to counterfeit medical products and similar crimes;
- Sanctions and aggravating circumstances;
- Collection, collation and analysis of data.

With regard to *prevention and training*, the report stresses as a good

practice that most State Parties have well-developed regulatory authorities that guarantee the quality, safety and efficacy of the medical products that they authorise for marketing. However, deficiencies exist in the area of training, such as lack of training for procurement programmes and the distribution of medical products as key areas for the effective fight against counterfeit medical products, especially during a pandemic. In addition, review programmes on the effectiveness of training measures and the training of specialised investigation teams on counterfeit medical products with specialised investigation techniques are largely non-existent.

Other key findings include:

- *Education*: Information of the general public and awareness-raising campaigns, in particular in view of avoiding procurement from unauthorised online sources, worked well. Evidence was lacking regarding encouragement by the State Parties of civil society to become engaged in delivering awareness-raising campaigns to the public, as was the extent of delivery by civil society of such campaigns.
- *Victim protection*: All State Parties ensure adequate protection for victims of falsified medical products.
- *Cooperation and information sharing*: Cooperation mechanisms are in place, albeit most are general and not specific to counterfeiting medical products. Effectiveness of cooperation mechanisms is generally not reviewed and contact points for information exchange are in place, but often their powers are fragmented.
- *Detection*: Measures to proactively detect counterfeit medical products and to prevent that these products reach patients are found inadequate in the majority of the State Parties. It is also regretted that no additional measures during a pandemic were taken in the field of detection.
- *Investigations and prosecutions*: The level of implementation of the

criminal offences under Arts. 5–8 of the MEDICRIME Convention as well as the liability of legal persons (Art. 11 of the MEDICRIME Convention) is satisfying. However, in many State Parties specialized prosecutors in the field of counterfeiting medical products and similar crimes involving threats to public health have not been established. This leads also to problems of case allocation. Positively highlighted is that in the majority of states all prescribed offences in Arts. 5–8 and 9 of the MEDICRIME Convention are investigated and not subject to a complaint.

■ *Sanctions and aggravating circumstances*: All States Parties ensure a sufficient level of implementing the provision on sanctions (Art. 12 of the MEDICRIME Convention); in particular, the domestic laws permit the seizure, confiscation and disposal, including the destruction of medical products and other materials and instrumentalities employed to the commission of the offences established in Arts. 5–8 of the MEDICRIME Convention. Most State Parties have also implemented the obligations set up by Art. 13 of the MEDICRIME Convention that indicates six aggravating circumstances which, in so far as they do not already form part of the constituent elements of the offence, may, in conformity with the relevant provisions of domestic law, be taken into consideration in determining the sanctions in relation to the offences established in accordance with the Convention. However, the approaches of implementation of Art. 13 are different. No Party reported the consideration as an aggravating circumstance the commission of offences under the MEDICRIME Convention during a pandemic.

■ *Data collection*: Data collection remains a low priority in the majority of the State Parties, limiting the assessment of the impact of counterfeit medical products. This is seen a critical issue, particularly during public health crises, such as the COVID-19 pandemic.

In the final part, the report provides a series of recommendations to strengthen the enforcement of the MEDICRIME Convention and to enhance public health protection. The importance of cooperation among all stakeholders, including civil society, is underscored. The report concludes that despite pandemic-related challenges, State Parties have stepped up efforts to raise public awareness about the risks of counterfeit medical products and the dangers of purchasing medicines, medical devices and other medical products from unauthorised online platforms. The Parties have developed legislation and measures in place in several critical areas, which apply equally to pandemic and non-pandemic situations alike. However, the absence of review mechanisms challenge the effectiveness of the measures, which becomes more critical in times of major crises, such as a pandemic. TW

## Terrorism

### Guide for Practitioners on the Use of Conflict Zone Information in Criminal Proceedings

On 2 February 2025, the Council of Europe published a practical guide on the use of information collected in conflict zones as evidence in investigations and prosecutions of crimes of terrorism and crimes against international humanitarian law committed in armed conflicts. The guide entitled “Com-

parative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings”, was prepared by the Council of Europe Committee on Counter-Terrorism (CDCT), and the International Institute for Justice and the Rule of Law (IIJ) under the support of the United States of America.

The document compiles experience from member states to the CDCT in identifying, obtaining, and sharing information and materials from conflict zones, and their use as evidence in criminal proceedings. It aims to provide guidance on how to use information from conflict zones effectively to advance justice and accountability, in accordance with national laws and relevant international human rights and rule of law standards. The following issues are addressed:

- Sources and types of information collected in conflict zones;
- Mechanisms to obtain and/or share information;
- Steps to analyse and use information.

An annex provides answers to practitioners on frequently asked questions in the context of information from conflict zones.

The Comparative Practices complements the Council of Europe Recommendation of March 2022 ([CM/Rec\(2022\)8](#)) which set up non-binding rules on the collection and use of information from conflict zones as evidence in criminal proceedings related to terrorist offences. The Rec-

ommendation called on CoE member states to translate and disseminate its content as widely as possible among competent State authorities and more specifically among those involved in the process of using information from conflict zones as evidence in criminal proceedings related to terrorist offences in accordance with the rule of law.

### CDCT Guidelines on Prosecution of Violent Extremism

On 26 February 2025, the Council of Ministers of the Council of Europe adopted [guidelines](#) that aim to enhance the prosecution of violent extremism conducive to terrorism. The guidelines were developed by the Committee on Counter-Terrorism (CDCT) and are addressed to national criminal justice authorities to understand how far-right and far-left groups operate, which strategies they follow and how the elements of terrorist offences can effectively be examined/proven during the various stages of the criminal process. The guidelines stress the importance of combating terrorism and violent extremism in line with human rights standards, as guaranteed by the European Convention on Human Rights.

Addressing the growing issue of threats and terrorist attacks by violent extremist groups is part of the [2023–2027 Council of Europe Counter-Terrorism Strategy](#). The guidelines build on the findings of the [2022 Council of Europe report on emerging terrorist threats](#).



# Articles

## Articles / Aufsätze

Fil Rouge

The contributions in this 2025 eucrim issue focus on specific reform challenges in the area of freedom, security and justice: strengthening EU policies against new threats and addressing shortcomings in the implementation of existing European instruments.

Against the background of a number of changing security risks and with a view to defining an updated, horizontal, strategic EU security agenda, *E. Sason, C. Monti, and P. Olivares-Martinez* provide the reader with an outline of recent security policy developments at the European Commission level. The Commission is calling for an integrated EU security approach “by design”, one that mainstreams different internal and external policy fields and requires increased governance efforts.

To achieve more efficient operational anti-fraud coordination at the national level and strengthened cooperation with OLAF, *M. Juric* proposes reinforcing the structure and architecture of the anti-fraud coordination services (AFCOS) in the Member States. They currently follow very heterogeneous approaches from one Member State to another and therefore do not yet provide equivalent added value ensuring effective protection of the EU’s financial interests.

The conference report by *G. Theodorakakou, and L. Jakobi* on strengthening the future of the European Public Prosecutor’s Office (EPPO) summarises recent reform discussions on how to address shortcomings in the EPPO legal framework, focusing on three topics: (1) the EPPO’s procedures for collecting transnational evidence, (2) the material scope of the EPPO’s competence, currently concentrating on PIF offences, and (3) the statutory independence of the EPPO’s prosecutors.

In light of the entry into force of the new EU Anti-Money Laundering/Combating the Financing of Terrorism package and the recently set up European Anti-Money Laundering Authority (AMLA) in Frankfurt, *K. Meskens, and J. Vanstappen* outline the legislative and administrative changes involved. They examine their impact on the future role of the Belgian national financial intelligence unit with regard to reporting, strategic analysis, and information exchange on money laundering.

Given the strong practical implications of common agricultural policies (CAP) fraud, *C. Cantisani and L. Ricci* present the results of recent comparative Pisa university research. The study concludes with concrete proposals to improve analytical methods for detecting fraud and irregularities concerning CAP funds and for further developing inter-authority information exchange strategies. *F. Lo Gerfo* analyses CAP fraud from the angle of administrative sanction schemes for over-declaration that have been in place over different periods. He criticises “yellow card” legislation, namely capping the administrative penalties for serious cases of over-declaration. His analysis demonstrates that this approach leads to a regressive penalty structure for surface-based aid rules, and concludes that this may hinder the proportionate and deterrent character of the sanctions and should be discontinued.

Building in particular on Directive (EU) 2024/1260 on asset recovery and a brief comparative analysis of non-conviction-based confiscation (NCBC) models in Switzerland, Italy, and the UK, *F. Teichmann* makes a specific reform proposal to close current confiscation enforcement gaps in German law. He proposes, *inter alia*, an *in rem* civil procedure for NCBC in Germany, in which the public prosecutor must demonstrate the “overwhelming probability” of illicit origin.

*R. Stephenson, J. Rinceanu, and M. Bovermann* critically comment on the 2024 EU Regulation on the Transparency and Targeting of Political Advertising (PAR), which aims to respond to the dangers and misuse of microtargeting, a sophisticated data-based method of online manipulation. The article aims to spark discussion about the complexities of digital media regulation. Lastly, developing concrete proposals for practical implementation of the “right to translation”, including rights to interpretation and translation as mandated by EU Directives 2010/64/EU and 2012/13/EU in criminal proceedings, *T. Reichmann* discusses different perspectives on translation and interpreting for courts and other judicial bodies in Germany.

*Dr. Lothar Kuhl*, Former head of unit and senior expert, Directorate for Audit in Cohesion, European Commission

# Security – A Firm Construct or an Undetermined Concept?

## An Outline of the EU's Current and Future Security Architecture

Elisa Sason, Cristina Monti and Pablo Olivares Martínez\*

The concept of security within the EU's legislative and policy framework has evolved significantly over the past few decades, adapting to shifting realities. Building on existing and overarching foundations, notably the EU Security Union Strategy, the European Commission recently presented a trio of initiatives that further frame the EU's approach towards security. Having begun with a focus on conventional threats, such as terrorism and organised crime, the EU's security approach has expanded to encompass cyberattacks, hybrid threats, and the protection of critical infrastructure.

This article gives an overview of the most prominent adopted initiatives that have shaped, shape and will shape the EU's security architecture. The authors argue that the concept of security can no longer be viewed in isolation and that it should be seen as intersecting with a wide range of different instruments, actions, and policy areas. The authors consider it essential to establish clarity regarding the EU's concept of security as well as its governance structures in order to develop an efficient approach towards tackling existing and future threats. Continuous attention and vigilance will need to be paid to ensure a coordinated and horizontal approach to protect EU security.

### I. Introduction

While the concept of security has always been high on the European Union's political agenda, it has become increasingly prominent in recent years. Different wars and crises, as well as rapidly evolving global events continue to unfold daily. The challenges to security and stability on the European continent are greater than at any time since World War II, and the need for clarity on the concept of security is particularly crucial now.

But what is security? And what should it mean for citizens to feel secure in the EU? According to the EU's Treaty on the European Union (TEU), the values of respect for human dignity, freedom, democracy, equality, the rule of law, and respect for human rights are the fundamental principles of the Union, with the ultimate goal of promoting these values and the well-being of its people – especially peace.<sup>1</sup> Taken with the Treaty on the Functioning of the European Union (TFEU), this underpins the Union's overarching objective of providing citizens with a high level of protection in the areas of freedom, security and justice.<sup>2</sup> At the same time, it is clear from the Treaties that national security is a sole responsibility of each Member State<sup>3</sup> and that separate rules apply for the development of the Union's common foreign and security policy. Furthermore, while the Treaties provide a good starting point, they do not offer a definition of the concept of security that could apply across the Union and its legislation and policies. As we will see, this is a significant deficiency, particularly at a time when security challenges are fast growing.

Based on the rules in the core treaties, the Union has adopted a tremendous amount of legislative and policy initiatives over the past several decades, with the goal of creating and strengthening the EU's area of freedom, security and justice. These rules provide common standards across the Union to combat serious crime, improve cooperation between police and judicial authorities, and enhance the Union's overall resilience against different types of attacks. While the traditional focus of the Union's actions in the area of security have focused on preventing terrorist attacks, protecting borders, and fighting organised crime, now shifting geopolitical interests and emerging new technologies demonstrate the need to apply a broader horizontal approach towards security. Providing citizens with security based on a comprehensive and enforceable framework is an endeavour requiring heightened attention to considerations far beyond the conventional justice and home affairs agenda. This means first recognising the inextricable links between the Union's external security and security within its own borders but also expanding our working understanding of the security concept to areas such as the economy, energy, digitalisation, public health, transport, and climate, and addressing them effectively in defence policy.

This article outlines initiatives taken by the EU to protect its security, notably under the umbrella of the EU's Security Union Strategy 2020–2025 (section II) and explains recently adopted initiatives in this area as announced by the Political Guidelines for the new European Commission 2024–2029 (section III). It also presents the views from other EU Institutions and actors in the area of security

(section IV), before concluding with a number of final considerations (section V).

## II. An Evolving EU Security Policy: From Internal Priorities to a Comprehensive and Silo-breaking Approach

Over the past decades, the evolution of the EU's security policy has paralleled the changing global threat landscape and the Union's commitment to safeguarding its citizens and core values. This is one of the youngest policy areas at the EU level, stemming from a gradual transition from informal collaboration among an expanding number of Member States to inter-governmental cooperation and then to further integration based on common laws and initiatives. The first EU internal security strategy, covering 2010–2015,<sup>4</sup> primarily focused on traditional internal security priorities, such as organised crime and terrorism; however, it also included natural and man-made disasters. This foundational phase provided the necessary coordination among EU Member States's push to tackle cross-border and cross-sectoral threats to which no single Member State could effectively respond on its own.

A series of high-profile terrorist attacks in subsequent years prompted a significant strategic shift in Member States' approach towards security. The European Agenda on Security 2015–2020,<sup>5</sup> under the guidance of Commissioner *Julian King*, emerged as a response to these threats and demonstrated the need for greater cooperation between national authorities, EU institutions, and various stakeholders, including the private sector. This agenda went beyond a conventional approach to security threats, paving the way for a Security Union concept. It marked a transition from the traditional focus on internal vulnerabilities to the recognition that modern security challenges are increasingly transnational and multifaceted.

The advent of the **Security Union Strategy 2020–2025**,<sup>6</sup> entrusted to Commission Vice-President *Margaritis Schinas*, took this shift further. This strategy was designed at the peak of the COVID-19 pandemic, and it was founded on four strategic pillars: (i) creating a future-proof security environment, ii) tackling evolving threats, iii) protecting Europe from terrorism and organised crime, and iv) building a robust European security ecosystem. The Strategy aimed to provide a holistic and comprehensive approach to security in an increasingly complex threat landscape marked by hybrid threats, disinformation, and increasing geopolitical volatility – with unprecedented challenges to EU values and democracies. It targeted areas where the

EU could bring added value to national efforts and placed a particular emphasis on cybersecurity, the protection of critical infrastructure, hybrid threats, and the nexus between internal and external security.

During its timespan, new initiatives were incorporated under the umbrella of the Security Union Strategy in response to a number of specific circumstances that could not have been foreseen when it was first designed. It was not only the Russian war of aggression against Ukraine and the deteriorating situation in the Middle East that required additional and more decisive actions but also rapid technological developments. This was true, in particular, for the newer areas of focus in the original Strategy (critical infrastructure, cybersecurity, and hybrid threats), and they have been intensified in response to severe events. Examples of these new initiatives include the Cyber Solidarity Act,<sup>7</sup> the anti-corruption package,<sup>8</sup> and measures to counter migrant smuggling.<sup>9</sup> Parallel to the overarching framework provided by the Security Union Strategy, the Commission adopted targeted strategies in key security domains, including counterterrorism,<sup>10</sup> organised crime,<sup>11</sup> drug trafficking,<sup>12</sup> and trafficking in human beings.<sup>13</sup> This multi-pronged approach reflects the understanding that modern security challenges are interlinked and that vulnerabilities in one area can have cascading effects on others. An example illustrating an integrated approach where physical and cyber threats are addressed in tandem is the measures taken to protect public spaces and entities providing essential services, which have been coupled with efforts to secure digital infrastructures.

Over 40 legislative initiatives under the umbrella of the Security Union Strategy were proposed by the Commission and successfully adopted by the co-legislators (European Parliament and Council) in 2020–2025.<sup>14</sup> Key legislative achievements concern the protection and enhancing of the resilience of critical infrastructure in the EU against physical and digital threats, with the parallel adoption of the Directives on Critical Entities Resilience (CER)<sup>15</sup> and Network and Information Systems (NIS2).<sup>16</sup> Together, and once fully transposed and implemented by Member States, these Directives will ensure that risks and vulnerabilities affecting entities in a range of key sectors, such as energy, transport, and space, are better addressed. With the adoption of the Cyber Resilience Act<sup>17</sup> and the Cyber Solidarity Act,<sup>18</sup> the EU has been a pioneer in creating a solid legal framework to reinforce the cybersecurity of products with digital elements and supply chains, to strengthen solidarity at the EU level in case of major cyber incidents, and to enhance its collective capabilities to detect, prepare for, and respond to these types of risks.

At the same time, more “typical” security areas, such as the fight against organised and serious crime, continued to receive attention under the Security Union Strategy, with pivotal legislation adopted to tackle cybercrime (notably the e-evidence package<sup>19</sup>), trafficking in human beings,<sup>20</sup> and environmental crime<sup>21</sup> as well as money laundering and terrorism financing.<sup>22</sup> The new rules on asset recovery and confiscation<sup>23</sup> should lead to higher rates of confiscation of criminal proceeds – currently stagnating at an estimated 2% of illicit proceeds<sup>24</sup> – and allow for a stronger focus on crypto assets. A related area of major importance to the Strategy concerned the improvement of cooperation between police authorities and their operational capabilities. No less than three initiatives branded as the “EU Police Cooperation Code” were adopted: the Regulation on Automated Data Exchange for Police Cooperation (Prüm II),<sup>25</sup> the Directive on information exchange between law enforcement authorities and Member States,<sup>26</sup> and a Council Recommendation on operational police cooperation.<sup>27</sup> Through timely and accurate implementation, these measures are expected to significantly step up law enforcement cooperation across Member States and grant police officers more modern tools by which to exchange information.

While advancing the work on the Security Union Strategy and following the return of war to the European continent, the **Strategic Compass**<sup>28</sup> of March 2022 presented an ambitious plan of action for strengthening the EU’s security and defence policy. With the objective of boosting the EU’s cyber defence capabilities, enhancing situational awareness, and coordinating the entire range of defensive options available, this Compass aimed for a heightened level of resilience, a better response to cyber-attacks, and enhanced solidarity as well as improved mutual assistance. Increasing emphasis has been put on improving the EU’s capacities to counter hybrid threats. In addition to mechanisms, such as the Foreign Information Manipulation and Interference (FIMI) Toolbox and the Cyber Diplomacy Toolbox to be better prepared for and respond to cyberattacks, the EU put in place the Hybrid Toolbox, which is now operational and is used to respond to the intensified hybrid campaign by Russia targeting the EU and its Member States. Moreover, the idea of deploying EU Hybrid Rapid Response Teams was developed to offer short-term, tailored support to Member States and partner countries. Also noteworthy is the fact that the Strategic Compass identified space as a fifth operational domain of warfare (alongside land, sea, air, and cyber domains) and proposed measures to improve the collective protection of space systems and services against threats.<sup>29</sup>

Central to the Security Union Strategy has been its focus on **implementation**, with the Commission adopting seven

progress reports to regularly report on progress achieved in the 2020–2024 period.<sup>30</sup> The final progress report<sup>31</sup> of the Strategy adopted in May 2024 concluded with an outlook on **security challenges beyond 2025**. Accessing data in cutting-edge technologies like quantum communication infrastructure, artificial intelligence, and advanced surveillance pose significant challenges, highlighting the need to continue exploring how law enforcement can make use of digital technologies, while also ensuring the full respect for fundamental rights and cybersecurity.<sup>32</sup> Indeed, the intersection of technology and security presents a growing paradox: we must protect data and technological advancements, in line with EU values and principles, yet these very assets can also be exploited by criminals for illicit activities.

The final progress report called for a fresh approach to the way EU institutions and bodies and Member States respond to challenges, guaranteeing the EU’s capacity to respond swiftly when necessary as well as avoiding silos and response mechanisms that duplicate risk assessment or complicate crisis response.<sup>33</sup> Here, the challenge lies in translating this into practical action within an increasingly complex security ecosystem, where multiple players with overlapping goals and responsibilities must navigate a delicate balance. The Joint Cyber Unit, identified by the Security Union Strategy as a crucial mechanism for coordinated and structured operational cooperation across the civilian, law enforcement, diplomatic, and defence communities serves as a prime example of how promising initiatives can lose momentum.

Finally, the progress report acknowledged that the Union’s understanding of the notion of security has broadened, as the risks facing the EU have multiplied. The need for Europe to become more autonomous and less dependent on third countries (be it in the area of technology or in the provision of critical products and services) brings with it a range of economic considerations situated at the interface between security and competitiveness. The report further emphasised that any modern approach to security must integrate both digital and cyber components and take international implications into consideration, while also ensuring that security is embedded in all EU policies and decision-making processes.<sup>34</sup>

### III. Current and Future Priorities

Extraordinary times call for extraordinary measures. This is also true for my Commission. To deal with the challenging way ahead, we need to switch into a preparedness mind-set. This is why, in the next weeks, I will convene the first-ever Securi-



ty College. This will ensure that the College members receive regular updates on security developments. From external and internal security to energy, defence and research. From cyber, to trade, to foreign interference. Only if we have a clear and in-depth understanding of the threats, including hybrid threats, can we effectively contribute to collective security.

Ursula von der Leyen, 9 March 2025

Given the current geopolitical context, it comes as no surprise that the notion of security is predominant in the Political Guidelines of Commission President *Ursula von der Leyen* during her second term of office.<sup>35</sup> In the Chapter “A new era for European Defence and Security”, she announced her vision for a new approach to crisis and security preparedness. Among the main initiatives listed in this section are the adoption of a Preparedness Union Strategy inspired by the 2024 Niinistö Report and a European Internal Security Strategy to ensure that security is integrated into EU legislation and policies by design. In line with this direction, President von der Leyen announced specific initiatives: to make Europol a truly operational police agency, to reflect on areas where the European Public Prosecutor’s Office’s (EPPO) mandate could be extended,<sup>36</sup> and to design a new EU action plan against drug trafficking, an EU Port Strategy with a strong focus on security, a new Counter-Terrorism Agenda, and a new European Critical Communication System – to be used by authorities in charge of ensuring security and safety.

The concept of the “Security College” was also announced by Commission President *von der Leyen* in a speech marking the first 100 days of her Commission’s mandate.<sup>37</sup> It aims to anchor security in the Commission’s policymaking, ensuring that the College of Commissioners receives regular updates on security developments in all policy areas.

The consolidation of security is also a red thread in the letters that Commission President von der Leyen sent to Commissioners-designate, setting their missions for this mandate.<sup>38</sup> First, Executive Vice-President *Henna Virkkunen* is responsible for the portfolio Tech Sovereignty, Security and Democracy, a title that implies a supervisory role in security policies, including internal security and defence. Furthermore, the Executive Vice-President is in charge of key security areas, such as cybersecurity. Second, Commissioner *Magnus Brunner* is responsible for Internal Affairs and Migration, focusing on the traditional aspects of security, such as the fight against terrorism and organised crime; he is also tasked with delivering on the Internal Security Strategy. Commissioner *Andrius Kubilius* is the first-ever appointed Commissioner for

defence. Preparedness, a policy closely linked with security, is included in the remit of Vice-President *Roxana Minzatu* and Commissioner *Hadja Lahbib*.

In her mission letters, Commission President *von der Leyen* calls on all Commissioners to draw on recent, high-profile reports addressing security policies. These include, in particular, the 2024 Draghi Report on the future of European competitiveness and the 2024 Niinistö Report on how to enhance Europe’s civilian and defence preparedness and readiness. The main security-related aspects of these reports and the linked initiatives adopted in this mandate, are described in the following sub-sections.

### Competitiveness as a prerequisite for securing prosperity and freedom

Presented on 9 September 2024, the Draghi Report on EU competitiveness<sup>39</sup> arrived at a crucial moment in the core mission of strengthening the Union’s competitiveness. With 176 concrete recommendations made in a range of sectors, the report is built on three key anchors: i) closing the innovation gap with the United States and China, particularly in advanced technologies; ii) a joint action plan for decarbonisation and competitiveness; and iii) increasing security and reducing dependencies from third countries.<sup>40</sup> Cutting regulatory burdens, using collective spending power in crucial areas such as innovation and defence, and applying stronger horizontal EU coordination are means to achieve these goals. Together with Enrico Letta’s 2024 Report on the Future of the Single Market,<sup>41</sup> Draghi’s steer is seen as key not only to reinvigorating the EU’s competitiveness but to safeguarding its economic security.

The European Commission responded with the adoption of the **Competitiveness Compass** on 29 January 2025,<sup>42</sup> setting out a roadmap with legislative and policy initiatives for the next five years to implement the recommendations of Draghi’s report. Based on the three key anchors identified by Draghi, the Compass introduces *transformational imperatives* to boost the EU’s productivity gap, particularly in the tech area, as a way to strengthen competitiveness. Preparedness and security are also part of the agenda; reference is made to new actions flowing from the joint White Paper on the future of European Defence, the Preparedness Union Strategy, and the Internal Security Strategy. Five enablers are guiding horizontal requirements for the implementation of the Compass across all policy sectors: i) simplifying the regulatory environment, ii) fully exploiting the po-

tential of the EU's Single Market, iii) providing financing through a Savings and Investments Union as well as a re-focused EU budget, iv) promoting professional skills and high-quality jobs and iv) improving policy coordination at the EU and national levels.

### Preparedness as a mindset and standard course of action

On 30 October 2024, former Finnish President *Sauli Niinistö* presented his report on strengthening Europe's civilian and military preparedness and readiness.<sup>43</sup> Aimed at informing future actions to be proposed by the High Representative for Foreign Affairs and Security Policy (in the following: High Representative) and the Commission in view of the Political Guidelines and mission letters to Commissioner-designates, this report is a clear wake-up call to the EU on the need for action, and it sets out a number of specific steps. The actions proposed relate to cross-cutting areas of strategic importance which include – but are not limited to – the EU's military capabilities, the provision of healthcare and building up sufficient stockpiles, the secure use and development of digital technologies, and the availability of critical raw materials and components. The Niinistö Report confirms the important link between security and competitiveness, underscoring Europe's need to be economically competitive – not only to keep itself and its businesses secure but also to make a real impact on international developments instead of merely adjusting to them.<sup>44</sup>

The Niinistö Report also underlines the need for the EU to consider and concretely prepare for worst-case emergency and crisis scenarios and to take more strategic responsibility in a world subject to constant change. The idea is to follow an integrated *whole of EU society* method, bringing together relevant stakeholders: national authorities, private entities, employers, trade unions, civil society organisations as well as – and perhaps most importantly – individual citizens. While the “whole of society” approach already made its appearance in the Security Union Strategy, its inclusion in future strategies remains relevant.

The ideas presented in the Niinistö Report were translated into the **European Preparedness Union Strategy**, adopted by the Commission and the High Representative on 26 March 2025.<sup>45</sup> The aim of this Strategy (accompanied by an action plan with 63 items and an indicative timeline for their implementation) is to establish a comprehensive framework ensuring the EU's preparedness to respond to any type of crisis, including climate change, health emergencies, natural disasters, and security infrastructure attacks. The Strategy is horizontal in nature, and it fosters a

culture of preparedness and resilience, thereby supporting the obligation of Member States under Art. 222 TFEU to act in solidarity in the event of crises. The actions proposed revolve around seven areas<sup>46</sup>, and include the development of an EU comprehensive risks and threats assessment. The latter will be done through the following: strengthening the Single Intelligence Analysis Capacity (SIAC); a future Climate Adaptation Plan; practical measures to increase preparedness of citizens to ensure self-sufficiency for a minimum of 72 hours; and the boosting of public-private cooperation and the EU-NATO partnership.

The Strategy also includes a section on ensuring the resilience of vital societal functions. Reference is made to the work carried out under the previous Commission mandate in the context of the Security Union as regards the protection of critical infrastructure and cybersecurity, in particular the adoption of the CER and NIS2 Directives. While it is not surprising that the Strategy calls for the urgent transposition of these Directives, it further envisages that the Commission will engage with Member States to identify additional sectors and services not covered by the current legislation where there may be a need to act, e.g., Europe's defence industrial base.<sup>47</sup>

A notable action put forward by the Strategy, also referred to in Niinistö's report, concerns the embedding of a *Preparedness and Security by Design* principle in future EU legislation, policies, and programmes. This approach slightly deviates from the recommendation put forward in the report, which called for an explicit security and preparedness check in all future impact assessments accompanying new legislative initiatives proposed by the Commission. Taken together with the principles of proportionality in combination with the Commission's objective in the Competitiveness Compass to simplify EU rules, the Strategy takes a more targeted approach, namely that future initiatives should be developed with preparedness and security perspective considerations in mind. The true value and implications of this approach will be revealed through practical application on a case-by-case basis in specific initiatives.

### Peace through defence?

A number of recommendations put forward by the Niinistö and Draghi reports particularly focused on defence. The response to these recommendations is evident in the **joint White Paper for European Defence Readiness 2030**<sup>48</sup> of the European Commission and the High Representative published on 19 March 2025. Against the background of the immense disruption of the post-Cold War political order currently taking place and the systematic under-in-

vestment in Europe's defence capabilities, the White Paper sets out a framework to strengthen European defence and to support Ukraine. The actual novelty of the White Paper is the launch of the ReArm Europe Plan, an urgent defence response plan with six measures to speed up defence spending in the EU: a new EU regulation to provide Member States with loans backed by the Union budget; a proposal to activate the National Escape Clause allowing Member States to mobilise additional defence expenditure, which could reach at least €800 billion over the next four years; additional incentives granting more flexibility and incentives to increase European defence investments; further contributions by the European Investment Bank, including a widening of the scope of defence-related funding; the mobilisation of private capital, including through the Savings and Investment Union; and the exploration of additional funding sources for defence, notably under the next Multiannual Financial Framework.<sup>49</sup>

With the objective of ensuring European defence readiness by 2030 at the latest, the White Paper provides concrete directions for invigorating the Union's defence technological and industrial base, stimulating research, and creating an EU-wide market for defence equipment. While Member States' defence spending has significantly increased over the years and is currently estimated at 1.9% of the EU's combined GDP (€326 billion in 2024),<sup>50</sup> it is still considered insufficient in the new era of security threats fuelled by geographical, geopolitical, technological, and competitive motives.

### ProtectEU: safeguarding the EU's internal security

The latest building block in the new security architecture designed by the Commission concerns the European Internal Security Strategy adopted on 1 April 2025.<sup>51</sup> Branded as "ProtectEU", this new strategy continues the foundational work laid out in the Security Union Strategy, despite use of the term "internal", and does not exclusively focus on the classical internal security threats (updating the Framework Decision on organised crime, strengthening Europol, and the adoption of new, targeted strategies and action plans in the areas of counterterrorism, and trafficking in firearms, drugs, and humans as well as the protection of children against crime). ProtectEU not only addresses threats posed by organised crime and terrorism but also puts the spotlight on hybrid threats, including incidents affecting the EU's critical infrastructure, cyber-attacks, disinformation, and foreign interference.

The Strategy of 1 April 2025 establishes a **new governance model** for European internal security.<sup>52</sup> This is done through consolidation of the principle that security should be main-

streamed in all the EU's future actions, in line with the Preparedness Union Strategy adopted at almost the same time. Regular meetings of the Commission Project Group on European Internal Security, enhanced by strategic cross-sectoral collaboration at the service level, should enable the Commission to embed the notion of security in all aspects of its work. The new format of the Commission's Security College will duly discuss internal security elements and their potential impact on different policy areas. To ensure the necessary transparency on progress made in implementing the actions put forward, the Strategy requires that the Commission regularly update the Council and European Parliament. Regular EU internal security threat assessments based on sectoral analysis should feed into the EU's comprehensive risk and threat assessment, as announced in the Preparedness Union Strategy.

The ProtectEU Strategy acknowledges that the online and offline dimensions of security have currently become blurred and puts a strong emphasis on digital risks and vulnerabilities, such as cybersecurity and cybercrime. In this context, the Commission also proposed an updated Cybersecurity Blueprint<sup>53</sup> on cybersecurity crisis management that, once adopted by the Council, would provide a solid framework for cyber crisis management. While it does not introduce new mechanisms and tools as such, it does present in a clear and simple manner how to make use of available mechanisms across the full crisis management lifecycle. The Action Plan on the Cybersecurity of Hospitals and Healthcare Providers<sup>54</sup> is another example of the need to accelerate collective action in particularly vulnerable areas. Moreover, the Strategy announces actions in the field of access to data by law enforcement, including the preparation of an impact assessment with a view to updating rules on data retention at Union level.

The Strategy reinforces that attempts to decouple internal and external security aspects are not feasible in the current context: threats originating outside the EU have a direct impact on the lives of European citizens. For example, drugs produced in Latin America and illegally trafficked to Europe end up in European cities and towns, thus inevitably increasing insecurity close to home. Geopolitical events, such as the new Taliban regime in Afghanistan and the fall of the al-Assad regime in Syria generate changes in drug trafficking routes and increase terrorist threat levels across Member States. Incidents in under-sea critical infrastructure in the Baltic States have the potential to disrupt a larger range of critical and essential services in Europe, such as energy supply and telecommunication services. In response to these latter incidents, the Commission and the High Representative presented

an Action Plan to enhance the security and resilience of submarine cables.<sup>55</sup>

#### IV. Views from other EU Institutions and Actors in the Area of Security

Shaping the EU's security is not a task which can be carried out by the Commission alone. Co-legislators, Member States' authorities and other actors including EU agencies and bodies operating in this area carry an important responsibility in materialising the EU's security architecture. This section provides an overview of their main positions.

The Council adopted in December 2024 strategic guidelines for the next five years in the area of freedom, security and justice<sup>56</sup>. The fact that these guidelines focus on implementation should not be seen as a lack of ambition, given the complexity and number of legislative and policy instruments adopted in recent years. The 39 guidelines provide useful insight into the Council's position in both a general and specific sense. For example, with regard to serious and organised crime, specifically the fight against corruption, the guidelines underline the continued need to focus on and implement the recommendations put forward by the High-level Group on access to data for effective law enforcement (e.g., the adoption of rules on data retention). In light of the EU's challenges related to the changing security landscape worsened by global conflicts and climate change, the guidelines also point out that initiatives in the Justice and Home Affairs area should contribute to strengthening preparedness and crisis response at Union level. With "Security, Europe" as its core motto, the Polish Presidency of the Council of the European Union had set this specific area at the heart of the EU's priorities.

In recent years, the European Parliament has adopted a number of resolutions reflecting its position on EU security. As co-legislator, it recently adopted a resolution on the White paper on the future of European defence.<sup>57</sup> Specifically, this resolution calls on the EU to invest substantially more in defence, to integrate a defence and security dimension in most Union policies,<sup>58</sup> and to embed a *Preparedness by Design* principle horizontally and consistently across EU institutions, bodies, and agencies. Earlier resolutions – following Commission strategies and actions in the area of organised crime,<sup>59</sup> cybersecurity,<sup>60</sup> and the Security Union Strategy<sup>61</sup> – offer further guidance on the Parliament's priorities. Having reflected on the new opportunities for fraud with EU funds following the COVID-19 pandemic (in connection to the disbursement of NextGenerationEU), the European Parliament also emphasised the

need to step up the fight against organised crime at the Union and national levels and called on the Commission to revise the Framework Decision on the fight against organised crime.<sup>62</sup> As regards the issue of funding, a visible difference exists between the Parliament's approach towards cybersecurity versus the traditional justice and home affairs policies. While for cybersecurity and related infrastructure deployment, the Parliament calls for a coherent use of EU funds and the need to exploit synergies between different EU programmes;<sup>63</sup> it expresses deep concerns and calls for adequate funding and staffing of EU Justice and Home Affairs agencies and bodies in order for the EU to deliver on the Security Union Strategy.<sup>64</sup>

EU agencies and bodies operating in the security sphere carry an important responsibility in forming future policy to prevent, anticipate, and respond to cross-border threats. Europol's most recent Serious and Organised Crime Threat Assessment report 2025<sup>65</sup> identifies cyber-attacks, online fraud schemes, (online) child sexual exploitation, migrant smuggling, drug trafficking, firearms trafficking, and waste crime as key threats. According to Europol, a particularly worrying and recent trend concerns the increased collaboration between criminal networks and hybrid threat actors. Guidance on the terrorism situation and trends in Europe is provided by, for example, the European Union Terrorism Situation and Trend Report.<sup>66</sup> Such terrorism and situation trend reports provide input for the future EU Counter-terrorism Agenda, which will need to reflect on the rise in terrorist attacks, the increased use of technological innovations such as Artificial Intelligence, and the active involvement of young individuals in terrorism and violent extremism. The increase in cyber-attacks and crimes committed through online means, notably ransomware and malware attacks, is also highlighted in the most recent ENISA Threat Landscape report.<sup>67</sup> All these agencies make an important contribution to shaping the EU's priorities in the area of security by raising situational awareness in their operational activities.

#### V. Conclusion

The increased attention to security across the EU, particularly in the current threat landscape, should be welcomed. However, the consolidation of the EU's cross-cutting approach to security has translated into a growing number of initiatives dealing with this topic, leaving the notion as open as it is salient.

In contrast with the previous Commission mandate, when the Security Union Strategy served as a comprehensive umbrella for the EU's security policy, there is currently no single



initiative to bring together all security matters. In addition to the recently adopted Preparedness Union Strategy and Internal Security Strategy, there are also sectoral strategies, such as those related to economic security, maritime security, and energy security. While the proposed initiatives raise security concerns to the highest political level, it remains to be seen how this will be organised in a clear and convincing way, ensuring streamlining and coordination.

An efficient legislative and operational environment, with enhanced clarity on the role, responsibilities, added value, and complementarities of the various actors in the security landscape, is indispensable and urgent. The operationalisation of the mainstreaming of security and preparedness into future EU policies and initiatives, as announced in the Preparedness Union Strategy and the Internal Security Strategy, may reveal how the EU's concept of security will be further framed. Such clarity is a prerequisite for the trust necessary when providing an integrated and holistic approach to existing and potential security challenges.

With the concept of security inherent to a wide range of different instruments, actions, and policy areas, there is a constant risk of overlaps, divergencies in interpretation, and a duplication of efforts that must be avoided if the EU is to live up to its responsibility under the Treaties to protect citizens. While certain areas (such as the protection of critical infrastructure) are recognised in multiple strategies, other areas (such as the dependencies on high-risk vendors for the provision of critical services, materials, technology, and equipment) have not received the same

concerted attention. Such gaps need to be addressed in a systematic way.

Stronger governance would also help address the challenge of funding for security policies and agencies, particularly in view of the upcoming negotiations on the next multiannual financial framework. A clear prioritisation and political will is needed to balance specific priorities, such as the strengthening of Europol and Frontex with new initiatives, e.g., the ReArm Europe plan to mobilise up to €800 billion for defence investment and the InvestAI initiative to mobilise €200 billion of investment in Artificial Intelligence.

Another point for consideration concerns the need to balance the work on preparing and negotiating new initiatives versus the need to timely and correctly implement agreed legislation. Without proper implementation and enforcement, legislative instruments and policies risk losing their impact in practice. Urgent political developments necessitate prompt adaptation and reaction at the EU and national levels. The EU level added value, and the merit of effective governance on these issues, thereby resides in ensuring stronger coordination, resource and intelligence pooling, increased collective efficiency, and a scale effect, building on Member States' efforts.

Ultimately, while security may not be better assured through the development of a firm construct or concept, vigilance remains of the essence for the EU in order to maintain a horizontal overview and ensure a coordinated approach towards the protection of its own security, especially in today's times.

---

\* The views expressed in this article are solely those of the authors and are not an expression of the views of their employer or the institution they are affiliated with.

1 Cf. Art. 2 TEU: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail." Art. 3(1) TEU: "The Union's aim is to promote peace, its values and the well-being of its peoples."

2 Art. 67(3) TFEU: "The Union shall endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws."

3 Art. 4(2) TEU: "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential

---

State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

4 Communication from the Commission to the European Parliament and the Council, *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Agenda on Security*, COM(2015) 185 final.

6 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions *on the EU Security Union Strategy*, COM(2020) 605 final.

7 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

8 On 3 May 2023, the Commission adopted a package with legislative and policy measures to strengthen the fight against corruption

(see also the news in *eu crim* 2/2023, 139–141). While the directive on combatting corruption is currently under trilogue negotiations by co-legislators, multiple actions proposed by the Joint Communication on the fight against corruption (JOIN(2023) 12 final) have been adopted, including the setting up of an EU Network against Corruption.

9 Proposal for a Regulation of the European Parliament and of the Council on enhancing police cooperation in relation to the prevention, detection and investigation of migrant smuggling and trafficking in human beings, and on enhancing Europol's support to preventing and combating such crimes and amending Regulation (EU) 2016/794, COM(2023) 754 final; Proposal for a Directive of the European Parliament and of the Council laying down minimum rules to prevent and counter the facilitation of unauthorised entry, transit and stay in the Union, and replacing Council Directive 2002/90/EC and Council Framework Decision 2002/946 JHA, COM(2023) 755 final.

10 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, COM(2020) 795 final.

11 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on the EU Strategy to tackle Organised Crime 2021–2025*, COM(2021) 170 final.

12 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *EU Agenda and Action Plan on Drugs 2021–2025*, COM(2020) 606 final.

13 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on the EU Strategy on Combatting Trafficking in Human Beings 2021–2025*, COM(2021) 171 final.

14 Communication from the Commission to the European Parliament and the Council *on the Seventh Progress Report on the implementation of the EU Security Union Strategy and Annex*, COM(2024) 198 final.

15 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022, 164.

16 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, 80.

17 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

18 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025.

19 For more information on the E-evidence package: A. Juszczak and E. Sason, "The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice – An Introduction to the New EU Package on E-evidence", (2023) *eu crim*, 182–200.

20 Directive (EU) 2024/1712 of the European Parliament and of the Council of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, OJ L, 2024/1712, 24.6.2024.

21 Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC,

**Elisa Sason**

Policy Coordinator, Secretariat-General,  
European Commission



**Cristina Monti**

Policy Coordinator, Secretariat-General,  
European Commission



**Pablo Olivares Martínez**

Policy Coordinator, Secretariat-General,  
European Commission



OJ L, 2024/1203, 30.4.2024. For details and comments on this Directive, see the articles in the special *eu crim* issue no. 2/2024 ("Protection of the Environment").

22 New rules to tackle anti-money laundering and terrorism financing (AML/CFT) together with the Regulation establishing the new Anti-Money Laundering Authority (AMLA) were published in the Official Journal on 19 June 2024. See also the news in *eu crim* 2/2024, 113–120.

23 Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, OJ L, 2024/1260, 2.5.2024.

24 Europol, *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, 2025, p. 26.

25 Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation), OJ L, 2024/982, 5.4.2024.

26 Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, OJ L 134, 22.5.2023, 1.

27 Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation, OJ L 158, 13.6.2022, 53.

28 Council of the European Union, *A Strategic Compass for Security and Defence – for a European Union that protects its citizens, values and interests and contributes to international peace and security*, Council document 7371/22 of 21 March 2022. Available at: <<https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>> accessed 10 June 2025.

29 Ibid, pp. 13, 23–24, 28, 32, 37, 44.

30 All seven progress reports on the implementation of the Security Union Strategy 2020–2025 are available here: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-of-life/european-security-union\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-of-life/european-security-union_en) accessed 10 June 2025.

31 Communication from the Commission to the European Parliament and the Council on the Seventh Progress Report on the implementation of the EU Security Union Strategy, COM(2024) 198 final.

32 Ibid, pp. 22–23.

33 Ibid, p. 24.

34 Ibid, p. 22.

35 Europe's choice. Political Guidelines for the next European Commission 2024–2029. Ursula von der Leyen, Candidate for the European Commission President. Published on 18 July 2024, available at: [https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648\\_en?filename=Political%20Guidelines%202024-2029\\_EN.pdf](https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf) accessed 10 June 2025.

36 During the past few years, there have been several suggestions from different stakeholders on areas to which the EPPO's competences could be extended. On 12 September 2018, the Commission adopted a Communication, including an initiative to extend the competences of the EPPO to cross-border terrorist crimes. See, for more information on this initiative: A. Juszcak and E. Sason, "Fighting Terrorism through the European Public Prosecutor's Office (EPPO)? What future for the EPPO in the EU's Criminal Policy?", (2019) *eucri*m, 66–74.

37 Press remarks by President von der Leyen on the first 100 days of the 2024–2029 Commission, 9 March 2025, [https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT\\_25\\_721](https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_25_721) accessed 10 June 2025.

38 An overview of the mission letters to Commissioners-designate can be found at: Commissioners-designate (2024–2029) – European Commission, [https://commission.europa.eu/about/commission-2024-2029/commissioners-designate-2024-2029\\_en](https://commission.europa.eu/about/commission-2024-2029/commissioners-designate-2024-2029_en) accessed 10 June 2025.

39 The Draghi Report: The future of European competitiveness, September 2024, available at: [https://commission.europa.eu/topics/eu-competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en) accessed 10 June 2025.

40 Ibid, p. 17.

41 Enrico Letta, *Much more than a market. Speed, security and solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, April 2024, available at: [https://single-market-economy.ec.europa.eu/news/enrico-letta-report-future-single-market-2024-04-10\\_en](https://single-market-economy.ec.europa.eu/news/enrico-letta-report-future-single-market-2024-04-10_en) accessed 10 June 2025.

42 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Competitiveness Compass for the EU*, COM(2025) 30 final.

43 Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness. Report by Sauli Niinistö, former President of the Republic of Finland, in his capacity as Special Adviser to the President of the European Commission, available at: [https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union\\_en](https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en) accessed 10 June 2025.

44 Ibid, p. 7.

45 European Commission & High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the *European Preparedness Union Strategy*, JOIN(2025) 130 final.

46 (1) Foresight and anticipation; (2) resilience of vital societal functions; (3) population preparedness; (4) public-private cooperation;

(5) civil-military cooperation; (6) crisis response coordination; and (7) resilience through external partnerships.

47 Niinistö Report, *op. cit.* (n. 43), p. 21.

48 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint White Paper for European Defence Readiness 2030*, JOIN(2025) 120 final.

49 Ibid, pp. 17–19.

50 Ibid, p. 16.

51 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on *ProtectEU: a European Internal Security Strategy*, COM(2025) 148 final.

52 Ibid, p. 3.

53 Proposal for a Council Recommendation for an EU Blueprint on cybersecurity crisis management, COM(2025) 66 final.

54 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *European action plan on the cybersecurity of hospitals and healthcare providers*, COM(2025) 10 final.

55 Joint Communication of the European Commission and High Representative of the Union for Foreign Affairs and Security Policy: *EU Action Plan on Cable Security*, JOIN(2025) 9 final.

56 Strategic guidelines for legislative and operational planning within the area of freedom, security and justice adopted at the Justice and Home Affairs Council on 12 December 2024, Council document 16343/24.

57 European Parliament resolution of 12 March 2025 on the White Paper on the Future of European Defence (2025/2565(RSP)), P10\_TA(2025)0034.

58 Ibid, point 9.

59 European Parliament resolution of 15 December 2021 on the impact of organised crime on own resources of the EU and on the misuse of EU funds with a particular focus on shared management from an auditing and control perspective (2020/2221(INI)), P9\_TA(2021)0501.

60 European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)), P9\_TA(2021)0286.

61 European Parliament resolution of 17 December 2020 on the EU Security Union Strategy (2020/2791(RSP)), P9\_TA(2020)0378.

62 Ibid, point 8: "reiterates its previous calls for the revision of Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, and the need to establish a common definition of organised crime; considers that this common definition should also take into account the use of violence, corruption or intimidation by criminal groups to obtain control of economic activities or public procurement, or to influence democratic processes."

63 European Parliament resolution of 10 June 2021, *op. cit.* (n. 60), point 7.

64 European Parliament resolution of 17 December 2020, *op. cit.* (n. 61), point 42: "Is deeply concerned by the lack of resources allocated to some EU agencies acting in the field of justice and home affairs (JHA) to comply fully with their mandate; calls for proper funding and staffing of EU agencies and bodies in the field of JHA in order for the EU to deliver on the Security Union Strategy."

65 Europol SOCTA, 2025, *op. cit.* (n. 24).

66 Europol (2024), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.

67 The ENISA Threat Landscape 2024 covered the period from July 2023 to June 2024 and was published in September 2024. The primary cybersecurity threats identified are: ransomware, malware, social engineering, threats against data, threats against availability: Denial of Service, information manipulation and interference, and supply chain attacks.

# The Role of an AFCOS in a New Anti-fraud Architecture

Mirjana Jurić

It goes without saying that the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO) form the heart of the protection of the EU's financial interests. However, the national authorities of the EU Member States are in the frontline when it comes to fighting fraud, bearing in mind that achievements in the field of the protection of the EU's financial interests also depend on the readiness and capacity of OLAF's and EPPO's partners in the Member States, (potential) candidate countries, and other non-EU countries, all of which cooperate to this end.

While the EPPO facilitates the achievement of its objectives in many ways through delegated prosecutors, OLAF, lacking a possibility to delegate its function, mainly relies on the anti-fraud coordination services (AFCOSes). These are established in each EU Member State to ensure effective cooperation and exchange of information with OLAF. In the absence of a stable legal framework for the role and mandate of an AFCOS, the challenges for cooperation with OLAF and also with other partner institutions are even greater.

This article tackles the issue of why it is necessary to better define the role and mandate of an AFCOS in the area of the protection of the EU's financial interests. A strengthened structure would enable the AFCOS to play a more significant role in the new anti-fraud architecture and in this way ensure, with improved capacities, better and more effective cooperation and partnership with the EU and relevant national authorities.

## I. Introductory Remarks

The EU is currently facing great challenges. Next to general developments, such as post-pandemic recovery, inflation, the war of aggression on Ukraine, etc., challenges are also evident in the context of financial crime: transactions have become digital, cross-border schemes are increasingly frequent and complex, and organised crime has continuously expanded its business into fraud against EU funds. Such threats put an enormous strain on the EU budget and require constant adaptation of the anti-fraud authorities to the changed modus operandi of fraudsters in order to stay ahead of the game. Therefore, certain adjustments in the anti-fraud architecture are called for.

While protecting the EU budget is a shared responsibility between the EU and its Member States, the European Commission plays a leading role in setting the standards and creating the (legal) framework for this shared responsibility. The time is ripe to review the efforts made by the European Commission in the area of the protection of the EU's financial interests and to give a new impetus to reform efforts.

The establishment of the EPPO aimed to improve the fight against crimes affecting the EU's financial interests and increase the effectiveness of the criminal law response to fraud in the participating Member States. OLAF's objective is to be a strong partner to the EPPO while maintaining its operational independence. Concretely, OLAF continues to act by conducting (administrative) investigations, with the possibility of issuing a judicial recommendation if the

EPPO has no jurisdiction, e.g., OLAF is at the forefront of anti-fraud action in cases not taken by the EPPO but requiring administrative action.

However, the achievement of goals in the area of the protection of the EU's financial interests requires much stronger cooperation, both with EU institutions and partner authorities in the Member States as well with players outside the European Union. In other words: in order to ensure that all available means are being used to fight fraud and corruption detrimental to the EU's financial interests in the future anti-fraud landscape, it is necessary to establish close relations with all players involved, both at the EU and national levels, while ensuring that their individual roles and mandates in this regard are clearly prescribed.

In this context, it is useful to consider where in the fight against fraud and the protection of the EU's financial interests the capacities of the anti-fraud coordination services (AFCOSes) could and should be used. Such considerations are all the more problematic in light of the currently rather limited mandate of the AFCOSes and also their insufficiently clear role in terms of purpose and added value for the national systems. The role of an AFCOS is still overshadowed by the importance of a number of other OLAF partner institutions and in relation to other EU and national institutions.

Against this background, this article will illustrate the role, mandate, and importance of designating AFCOSes as OLAF's partners in Member States for the purpose of the protection of the EU's financial interests. Recommenda-



tions will be made for the future evolvement of AFCOSes within a sufficient legal framework.

## II. Development of AFCOS and its Role and Mandate in the Protection of the EU's Financial Interests

Initially, Member States had no legal obligation to establish an anti-fraud coordination system or an anti-fraud coordination service. The legal obligation for Member States to “designate” an AFCOS was assigned to the Member States in 2013 with the adoption of the OLAF Regulation (Regulation 883/2013).<sup>1</sup> In 2020, within the framework of the most recent amendments to the OLAF Regulation, the AFCOS provision required improvement in terms of a better understanding of the mandate of an AFCOS in relation to its cooperation with OLAF. In this regard, Art. 12a of Regulation 2013/883, as amended by Regulation 2020/2223,<sup>2</sup> stipulates that EU Member States are required to designate an AFCOS to facilitate effective cooperation and exchange of information with OLAF, including information of an operational nature, and to provide or coordinate the necessary assistance for OLAF to be able to carry out its tasks effectively.<sup>3</sup>

However, the Union legislator also clarified that the organisation and powers of the AFCOS are left to each Member State.<sup>4</sup> Thus, the EU legal framework gives the Member States autonomy in deciding where to designate the AFCOS within their national administrative structures. The Union legislative framework is quite general and insufficiently clear in respect of the Member States’ obligation to protect the financial interests of the EU and the tasks of an AFCOS, which can be interpreted in different ways in each Member State. This has led to significantly different AFCOS models and thus to major differences in the national legal frameworks that regulate both the protection of the financial interests of the EU as well as the structure, role, and mandate of an AFCOS. Consequently, the current situation also leads to different working results by AFCOSes, i.e. outputs and deliverables.

What is also striking: The provisions within OLAF Regulation 883/2013 regulating the obligation for Member States to designate an AFCOS significantly deviate from the criteria for the designation of an AFCOS that the acceding EU Member States – concretely, Romania, Bulgaria, and Croatia – had to fulfil with respect to specific benchmarks in the accession negotiation chapters. The EU requested the acceding Member States to establish a “strong” legal and institutional framework for their AFCOSes while at the same time not imposing the same standards on the long-standing

Member States.<sup>5</sup> Therefore, the model, role, and mandate of the established AFCOSes in these recently joined Member States are significantly different than those of the established Member States, which were not required to meet such criteria. This also resulted in greater administrative burdens and workload in the new Member States (Croatia, Bulgaria, and Romania).<sup>6</sup>

For example, during the accession process, Croatia received benchmarks from the European Commission to fulfil through Chapter 32 – Priority 4. These benchmarks were based on recommendations provided to Croatia by OLAF, following a thorough analysis of mechanisms that Croatia’s competent institutions had for the protection of the EU’s financial interests. In this sense, the analysis was not conducted only at the level of the authorities responsible for the financial management and control system but also at the level of bodies with “repressive functions” (in Croatia, these bodies are referred to as AFCOS network bodies: State Attorney’s Office, Ministry of Interior, Customs and Tax Administrations, Sector for Financial and Budget Supervision, etc.). Upon finalisation of the analysis, Croatia received very clear recommendations and benchmarks to be fulfilled in order to successfully close the negotiation chapter. As a result, the Croatian AFCOS unit has a much broader scope of mandate and tasks than it would have had taking into consideration only Art. 12a of the above-mentioned Regulation 883/2013 as amended by Regulation 2020/2223.<sup>7</sup>

Another aspect in the discussion is that OLAF’s potential efforts in terms of harmonising the role and mandate of AFCOSes at the level of the Member States have unfortunately not been clearly visible since 2013. In this context, it was for instance not visible at any level that the European Commission and OLAF consider an AFCOS to be an important and serious partner in the protection of the EU’s financial interests and denote an improvement in anti-fraud policies. An AFCOS was instead seen as a provider of necessary information and a contact point or connector to the competent national institutions. This is corroborated by the fact that the amendments to the OLAF Regulation have not made any significant contribution to a better understanding of the possible role and mandate of an AFCOS and its positioning in the new anti-fraud architecture, as outlined above. In the period from 2011 to 2017, the anti-fraud policies advocated by OLAF were primarily aimed towards the establishment of the EPPO. Key future actions to improve OLAF’s mandate and capacities were far less visible and recognized, including the importance of AFCOSes in the changing anti-fraud landscape.

The considerable discrepancy between the roles and mandate of AFCOSes in the various Member States, ranging

from “very ambitious” AFCOSes to AFCOSes that were granted only a minimal competence, became even more obvious in 2020 after the adoption of amendments to the 2013 OLAF Regulation and the start of implementation of the provisions of Art. 12a. On the one hand, observers had the impression that anti-fraud coordination services exclusively work for OLAF and provide no added value to national systems. On the other hand, the question arose as to why OLAF imposed much larger obligations on the candidate countries (within the negotiation chapters related to the protection of EU financial interests) than to long-standing Member States, even though an adequate EU legal framework for the designation and mandate of AFCOS is non-existent. Thus, it is important to assess:

- whether or not the Member States have regulated the role and mandate of their AFCOSes in accordance with OLAF’s expectations;
- whether or not cooperation between AFCOSes and OLAF is satisfactory and
- what the weaker areas are in which OLAF sees room for improvement.

In addition, the increasing assumption of additional tasks by OLAF beyond the protection of the EU’s financial interests (e.g., the protection of the environment)<sup>8</sup> have opened up a discussion on the need for a clearer description of OLAF’s mandate as well as the obligations of Member States in this regard, including the obligations of AFCOSes.

### III. Challenges and Open Issues

Having worked as an expert in the field of the protection of the EU’s financial interests for many years, I have noticed that the EU position on the role, model, mandate, and importance of AFCOSes has changed with each change in OLAF’s Director-General and the different priorities laid down by them during their mandates. An example of this is the approach towards the “Guidance note on main tasks and responsibilities of an Anti-Fraud Co-ordination Service (AFCOS)” promoted by OLAF’s first Director-General, which was updated in 2002, 2011, and 2013.<sup>9</sup> This document was considered to be OLAF’s political vision according to which direction the role, model, and mandate of an AFCOS was to be developed. However, it was never properly transposed into binding provisions within EU legislation for the protection of the EU’s financial interests. OLAF’s activities on the need to harmonise the model and role of an AFCOS with those Guidelines at the level of the Member States ceased in 2013; today, we can look back on a long period of different approaches and policies that each succeeding Directors-General pursued during his

mandate, leading to different interpretations on AFCOSes for many years.

Defining the role and mandate of AFCOS as well as its position in cooperation with EU and national authorities should not, however, be left to the approaches/policies pursued by OLAF’s Director-Generals. Instead, a consistent EU legal framework that guarantees clear and stable provisions for an AFCOS must be created. Against this background, the question emerges as to whether or not the comprehensive EU legislative framework relevant for the protection of the EU’s financial interests should be further amended in order to significantly improve AFCOS issues in areas of perceived weaknesses. I wish to point out three requirements:

- We need a clear vision on the part of the European Commission and OLAF on what exactly is expected from AFCOSes and whether or not the existing AFCOS models meet their expectations, taking into account the existing, significantly different AFCOS models and, consequently, significant differences in the quality and quantity of their deliverables.
- It is necessary to duly assess the justification of the establishment of an AFCOS in order to answer the question of whether it only exists for the purpose of providing logistical assistance to OLAF and possibly also some other EU institutions/bodies in the future, or whether it also provides added value to the national administrative structure (in light of the fact that AFCOS employees are not employees of OLAF but of relevant national institutions).
- We must use the experiences gained in the process of establishing the EPPO and in view of its functioning, which includes the delegation of its functions to the delegated prosecutors in the Member States. In doing so, we can see whether or not the AFCOSes can appropriately play a more significant role in the new anti-fraud architecture and ensure better cooperation and partnership with the EU and national authorities with enhanced capacities.

### IV. Conclusion

In order to strengthen the architecture designed to effectively fight fraud to the detriment of the EU’s financial interests and to develop new tools for this purpose, further development of the anti-fraud policies at the EU level is of utmost importance. In the process, it is important that the European Commission, among other things, takes a clear political position on the future role and mandate of each AFCOS as one of OLAF’s key partners and its possible positioning in the new anti-fraud architecture. This position will not only contribute to strengthening the capacity of OLAF

but also guarantee more effective cooperation and partnership with the EU and national authorities.

This is the only way to improve the institutional and legal framework for the protection of the EU financial interests at the level of the Member States. Given the evaluation process for the administrative and criminal legal framework for the protection of the EU's financial interests, we currently have the opportunity to significantly improve anti-fraud policies and, in turn, the entire legal framework for the pro-

tection of the EU's financial interests. This approach would also greatly contribute to re-gaining citizen's trust in EU and national institutions and their genuine political will to fight fraud and corruption at all levels.

There is no alternative to clearly setting political goals and striving towards a consistent, clear, and stable EU institutional and legal framework in the future. Getting out of the comfort zone is important for all institutions and players involved if they wish to make significant strides in this area.



**Mirjana Jurić**

Head of AFCOS Unit, Ministry of Finance of the Republic of Croatia, Directorate for Financial Management, Internal Audit and Supervision

1 Art. 3(4) of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, 1.

2 See Art. 1(13) of Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, OJ L 437, 28.12.2020, 49.

3 See also Recital 37 of Regulation 2020/2223.

4 Ibid.

5 On the different development of obligations to designate AFCOSes between "new" and "old" Member States, see also L. Jellínek and C. Kreith, "Protecting EU Taxpayer Money together with Global Partners – 25 Years of International Relations of the European Anti-Fraud Office", (2024) *eu crim*, 324, 330–1.

6 One example is that Croatia invested much more human and financial resources in its AFCOS than the "established" Member States.

7 For example, the tasks of the Croatian AFCOS include the following:

- Coordinating drafting the national anti-fraud strategy;
- Initiating amendments to the legal framework related to the protection of the EU's financial interests;
- Coordinating irregularity and fraud risk assessment at the level of the AFCOS system;
- Ensuring timely reporting of irregularities to OLAF by implementing irregularity management procedures, administering the irregularity management system at the national level (including user support), and ensuring the technical accuracy of irregularity reports;
- Planning and organising training activities related to the protection of EU funds;
- Facilitating the exchange of information with OLAF;
- Providing support to OLAF during on-the-spot checks on the territory of the Republic of Croatia;
- Conducting administrative checks on EU-funded projects.

8 See, for instance, OLAF's tasks for waste management as introduced through Regulation (EU) 2024/1157 of the European Parliament and of the Council of 11 April 2024 on shipments of waste, amending Regulations (EU) No 1257/2013 and (EU) 2020/1056 and repealing Regulation (EC) No 1013/2006, OJ L, 2024/1157, 30.4.2024. For OLAF's role in this context, see S. Grassin and L.I. Garruto, "Fighting Waste Trafficking in the EU: A Stronger Role for the European Anti-Fraud Office", (2024) *eu crim*, 143–145.

9 For the 2013 version, see ARES(2013)3403880, available at: <[https://poise.portugal2020.pt/documents/10180/19827/Guidance+Note+on+Main+Tasks+and+Responsibilities+of+an+Anti-Fraud+Coordination+Service+\(AFCOS\).pdf/0c438f5b-8056-4aa7-ae37-f13fef5f4ba8](https://poise.portugal2020.pt/documents/10180/19827/Guidance+Note+on+Main+Tasks+and+Responsibilities+of+an+Anti-Fraud+Coordination+Service+(AFCOS).pdf/0c438f5b-8056-4aa7-ae37-f13fef5f4ba8)>, accessed 12 February 2025.

# Strengthening the Future of the EPPO

## Notes on a conference at Villa Vigoni, Lake Como, Italy, 31 March – 2 April 2025

From 31 March to 2 April 2025, Villa Vigoni, part of the German-Italian Centre for European Dialogue, was the setting for a high-calibre exchange on the state and future of the European Public Prosecutor's Office (EPPO) and its underlying legal framework. Experts from the EPPO, scholars, and representatives from national governments and the European Commission convened to discuss the implementation and impact of the EPPO Regulation, the effectiveness and efficiency of the Office, and its working practices. This conference report summarises the presentations held by legal experts as well as the exchange of ideas and discussions, which were inspired by the beautiful setting of Villa Vigoni at Lake Como.

### I. Conference Opening

The conference was opened by the hosts of the conference, Prof. Dr. *Dominik Brodowski*, LL.M. (UPenn) (Professor for Europeanization, Internationalization and Digital Transformation of Criminal Law and Criminal Procedure at Saarland University, Germany) and Dr. *Sebastian Trautmann* (European Delegated Prosecutor from Cologne, Germany).

In her keynote speech, **Laura Codruța Kövesi**, the European Chief Prosecutor (ECP), emphasised three strategic priorities, which are essential for the effective operation of the European Public Prosecutor's Office (EPPO): its independence, the scope of its competence, and the relationship between the ECP and the College and Administrative Director of the EPPO. She stressed that the Office is a judicial body and must be recognised and treated as such, particularly regarding budgetary matters and appointment procedures for prosecutors. Kövesi expressed concern about potential threats to the EPPO's independence, highlighting risks associated with national government influence in the appointment process of European Prosecutors and European Delegated Prosecutors (EDPs). She also noted cooperation difficulties with national authorities supporting the EDPs' work, which could further compromise the EPPO's independence. In her conclusions, Kövesi advocated for an extension of the EPPO's competence to encompass criminal offences for the violation/circumvention of EU restrictive measures and called for greater clarity regarding the Office's competence in corruption-related crimes and "inextricably linked offences".

### II. Acquisition and Use of Evidence

The first panel focused on the acquisition and use of evidence. It was opened by **Dr. Hans-Holger Herrnfeld** (Retired Senior Federal Prosecutor (Germany); former Head of Division at the German Federal Ministry of Justice) who gave an analysis of Art. 31 of the EPPO Regulation. He proposed concrete amendments to this provision aligned with the recent ruling by the European Court of Justice (ECJ) in case C-281/22 (*G.K. and Others [parquet européen]*). He noted, however, that the ruling left several questions unresolved. The ensuing discussion primarily revolved around judicial review mechanisms in cross-border investigations, namely whether or not it is more desirable to establish a "single authorisation system". The participants also debated whether harmonisation of *ex ante* judicial review should apply solely to cross-border cases or extend also to domestic procedures, such as searches and seizures, where divergence exists in the laws across the EU. Some participants argued for assigning the competence for *ex ante* judicial authorisation to the ECJ or to the EPPO's Permanent Chamber, with both proposals facing criticism.

**Prof. Dr. Michele Caianello** (Professor at the University of Bologna, Italy) and **Isadora Neroni Rezende** (PhD Candidate at the University of Bologna, Italy) dealt with the flow of evidence across borders and described Art. 37 of the EPPO Regulation (the provision on the admissibility of evidence) as being outdated and not sufficiently proactive. They recommended amending the provision to include flexible exclusionary rules addressing violations likely to compromise evidence integrity, such as breaches of the right of access to a



lawyer. The discussants generally favoured strengthening rules around investigative measures, including judicial authorisation and defence rights, rather than focusing on rules regarding evidence admissibility. *Caianello* and *Rezende* emphasised that rules governing ex ante judicial authorisation, defence rights, and admissibility of evidence each serve distinct purposes and suggested the necessity to address all three aspects comprehensively.

**Prof. Dr. Katalin Ligeti** (Professor of European and international criminal law at the University of Luxembourg) and **Dr. Sebastian Trautmann** analysed Art. 42 of the EPPO Regulation – the provision on judicial review. *Ligeti* highlighted that Art. 42 grants significant discretion to Member States in shaping judicial review of EPPO procedural acts, leading to a variable geometry across the Member States' rules. She recommended revising the article to establish common standards for the extent of judicial review and procedural acts, but she also acknowledged the challenges involved in harmonising specific modalities of judicial review. *Trautmann* emphasised the challenges arising from the specific nature of the EPPO, notably its cross-border investigations and the absence of direct judicial review of internal decision-making processes at the central level; he questioned whether the existing provisions sufficiently guarantee effective judicial protection or not. He was cautious about extensive harmonisation, expressing concern about potential discrepancies between EPPO cases and domestic criminal cases. In the subsequent discussion, several proposals were also made with regard to enhancing the efficiency of judicial review, such as the expansion of the ECJ's power to review EPPO procedural acts and EPPO's competence to directly refer preliminary questions to the Court – an idea that representatives from the EPPO welcomed.

In the final talks of the first panel, **Prof Dr. Liane Wörner, LL.M. (UW-Madison)** (Professor for Criminal Law, Criminal Procedural Law, Comparative Law, Medical Criminal Law and Legal Theory at the University of Konstanz, Germany) and **Luis Jakobi** (Research assistant at the chair of Prof. Wörner) provided an input on the provision on defence rights in the EPPO Regulation (Art. 41). In her presentation, Wörner emphasised the difficulties defendants face, due to the inherently transnational nature of EPPO investigations and the lack of uniform standards and dedicated rights for cross-border

investigations. She argued that the ECJ ruling in case C-281/22 introduced complexities detrimental to defendants; she advocated for stronger protection for defendants and recommended enhancing the ECJ's judicial review powers over EPPO procedural acts to promote greater uniformity within the context of EPPO's investigations. Further discussions explored issues regarding defendants' access to case files, digital evidence, and evidence gathered by EPPO staff.

### III. Competences and the Exercise of Competences – Conflicts, Clarifications, and Extensions?

In the second panel, legal experts debated questions on the EPPO's competences and their exercise. **Dr. Anneke Petzsche, M.Sc. (Oxford)** (Research assistant at the Humboldt University Berlin, Germany) reflected on the most important criteria for the expansion of the EPPO's competences in certain areas. According to *Petzsche*, violations of EU restrictive measures (recently enacted on occasion of Russia's war of aggression against Ukraine) are a particular concern, and there are doubts regarding offences of terrorism. In any case, the EU must focus on genuine European legal interests. Other areas could be regulated according to the complementary principle, so that the EPPO only intervenes if a Member State is unwilling or unable to prosecute.

**Cécile Soriano** (European Delegated Prosecutor from France) contributed that, in her view, there are three areas with political momentum in favour of an extension: environmental crimes, violations of restrictive measures, and corruption crimes. In the discussion, it emerged that Art. 22(4) of the EPPO Regulation represents an area of conflict with regard to the competence of the EPPO (criminal offences in respect of national direct taxes, including inextricably linked offences). The territorial competence provided in Art. 23(a) of the Regulation in its current version is also not sufficiently precise, e.g., in cases in which non-participating Member States and third countries are involved or if the offence is against the budget of the Union itself. In general, the discussion revealed that an extension of competences is primarily a political issue, as such a fundamental reform of the legal framework also entails risks to the current state of the EPPO Regulation and would require additional resources and staff for the Office.

**Luca De Matteis** (Head of Legal Service, EPPO) probed the logic behind Art. 25 of the EPPO Regulation and particularly its paragraph 3, one of the most challenging provisions in his opinion. In a necessary revision, clear criteria must be defined as to when multiple offences must be dealt with together in one procedure (inextricably linked offences). In the case of a unitary prosecution, it should be foreseeable, based on well-defined and clear criteria in paragraph 3, whether the EPPO or national authorities are competent. In a decision on competence, the rights of the accused must also be taken into account, especially as to whether or not they should have the right to challenge the decision on competence. In relation to Art. 27 of the EPPO Regulation (right to evocation), past practice shows that the deadline for evocation is not feasible. Ultimately, an effective implementation of the shared competence model between the EPPO and national authorities is required. In the exchange of opinions that followed, the problems with interpretation of Art. 25(3) of the EPPO Regulation were confirmed, with participants explaining that the provision reflects a compromise made with reluctant Member States, especially since not all current problems had been foreseeable at the time of drafting. It was also emphasised that Art. 27 of the EPPO Regulation is a “soft provision”, due to its lack of clarity, and therefore leads to ambiguities in practice.

**Prof. Dr. Luca Pressacco** (Assistant professor of Criminal Procedure at the University of Trento, Italy) addressed the matter of conflicts with national competences. He asserted that Art. 25(6) of the EPPO Regulation represents a problematic starting point, as it leaves decisions on Union law up to the Member States. Two possible views were discussed in this regard: first, the provision reflects the Member States’ unwillingness to give up competences; second, it simply confirms the hybrid structure of the EPPO itself. However, Art. 25(6) of the EPPO Regulation has also raised many questions regarding its substance; practice shows that, in particular, procedures involving special investigation bodies and political influence lead to problems with conflicts of competence. It was stressed that these issues require a solution. The discussion underscored that granting national authorities the competence to solve conflicts of competence between the EPPO and national authorities was a kind of trade-off to convince Member States to accept the broader competences provided in Art. 22 of the EPPO

Regulation. Likewise, the question of whether and to what extent the defendant should have a possibility to challenge a decision taken under Art. 25(6) of the EPPO Regulation, e.g., by way of a preliminary ruling, was discussed in depth.

In her contribution, **Georgia Theodorakakou** (PhD Candidate, University of Luxembourg, Luxembourg) addressed the extension of the investigation measures and other measures under Art. 30 of the EPPO Regulation. She highlighted several challenges in the current framework, particularly regarding the freezing of assets and the interception of telecommunications. These issues stem from a lack of harmonisation across Member States and the unavailability of certain measures in Member States in which they require the initiation of a judicial investigation by an investigating judge. She concluded that merely extending the list of measures under Art. 30 would be insufficient. Instead, existing problems must first be resolved. For instance, the role of the investigating judge needs clarification, and the procedures governing certain investigative measures should be harmonised – either beyond the EPPO’s investigations or only within them. A key issue raised in the discussion was the risk of double standards arising between domestic cases and EPPO cases if investigative measures are harmonised, along with the broader implications this might entail particularly for the position of the defendant and the principle of non-discrimination between EPPO and purely national proceedings.

#### IV. Institutional Independence and Sustainability

The third and last panel focused on questions of institutional independence and sustainability. **Lorenzo Salazar** (Senior Advisor on International Cooperation in Criminal Matters; Deputy Prosecutor General to the Court of Appeal of Naples (retired)) put forth that institutional independence within the EPPO is concretised through different mechanisms, such as the appointments of the European Chief Prosecutor, European Prosecutors and European Delegated Prosecutors (EDPs), the EPPO’s budget, and the status of EDPs. He suggested various measures to reinforce independence within the EPPO, such as applying the budgetary procedures used for EU institutions to the EPPO, revising status of EDPs, and enhancing cooperation with the staff supporting EDPs at the national level.

The following discussion highlighted issues related to EDPs' career progress, with proposals for establishing permanent EDP positions receiving mixed reactions. Some participants expressed concern about the risk of creating an overly independent EPPO, while others pointed to existing mechanisms (such as accountability, judicial review and dismissal procedures) that serve to balance and control the EPPO's independence.

With regard to the EPPO's accountability, **Marius Bulancea** (Head of Operations and College support Unit, EPPO) explained that the EPPO Regulation lacks clarity on how this is operationalised and questioned whether the current oversight mechanisms allow for a meaningful assessment of the EPPO's activities. He underscored that the EPPO's judicial nature necessitates distinct accountability mechanisms compared to other EU agencies, cautioning against performance metrics that overlook broader considerations. The subsequent discussion explored methods to accurately measure the EPPO's effectiveness and enhance accountability mechanisms.

In the next contribution, **Dr. Garonne Bezjak** (Head of Unit "European Public Prosecutor's Office; European Criminal Law policy", Federal Ministry of Justice and Consumer Protection, Germany) pointed out pressing concerns regarding the selection, status, and number of EDPs and support staff from the perspective of the Member States. For example, the Member States may be reluctant to agree to a much-needed increase in the number of EDPs because they may have to let their best prosecutors go, especially given the limited number of qualified applicants. Further complications for the EDPs' career progression arise from the double hat system, under which the EDPs serve as special advisors (Art. 96(6) of the EPPO Regulation). In addition, *Bezjak* stressed the need to address the current, unequal distribution of resources and staffing available to the EDPs, both within and between Member States. She concluded that many of these problems stem from the hybrid structure of the EPPO. In the ensuing discussion, it became clear that the double hat system poses several problems, yet some participants acknowledged its practical necessity. Several proposals were also discussed to reduce the disparities among EDPs, whether by strengthening the centralised, institutional level of the EPPO or the decentralised level in the Member States, and who should be responsible for the strengthening (particularly financially).

With his final input, **Prof. Dr. Dominik Brodowski** focused on the EPPO's independence from and through legal review. One key question is the extent to which the defence should have access to the decisions of the Permanent Chambers – in the interest of transparency – and to what extent these decisions should be subject to judicial review. Further questions arise in relation to Art. 113(4) of the EPPO Regulation regarding the responsibility for compensation for lawful yet unwarranted acts, whereby the protection of the EDPs from this responsibility is necessary in the interest of independence. In terms of independence through judicial review, *Brodowski* stated that it would be in the EPPO's interest to have more cases brought before the ECJ. However, the EPPO currently lacks the competence to submit preliminary questions to the ECJ. In the discussion, it was pointed out, on the one hand, that the decisions of the Permanent Chambers are published in accordance with Art. 10(8) of the EPPO Regulation; but the lack of public hearings, direct appeals, and the timing of access to these decisions were identified as problematic. On the other hand, it was acknowledged that a kind of non-public, internal deliberation within a prosecution office is not uncommon across legal systems and may be indeed necessary. It became clear that the role of the Permanent Chambers and, consequently, the general significance of their decisions need further clarification. Moreover, several questions were raised with regard to the involvement of the ECJ and its potential role in judicial review of the EPPO's procedural acts.

## V. Summary

The conference revealed that the functioning of the EPPO has exposed several shortcomings in the current text of the EPPO Regulation. These can be broadly categorised into three – albeit interrelated – areas:

- Certain provisions require clarification to ensure legal certainty; notable examples include the role of the investigating judge and the mechanisms for judicial review in cross-border investigations.
- Some provisions are dysfunctional and hinder the EPPO's operational efficiency and independence, thereby necessitating urgent amendments; this applies in particular to rules governing the status of European Delegated Prosecutors, the appointment procedure for European Prosecutors,

the exercise of the EPPO's competences, and the resolution of competence conflicts with national authorities.

- There is a need to reinforce the protective dimension of EPPO investigations by enhancing procedural safeguards for individuals involved in its proceedings and by ensuring effective judicial review of the EPPO's procedural acts.

Against this background, the forthcoming edited volume on the conference will surely be a contribution rich in ideas and inspiration for the upcoming course

of review of the EPPO Regulation 2017/1939, which is scheduled to begin in the second half of 2026.

*Georgia Theodorakakou*

Doctoral researcher, University of Luxembourg, Faculty of Law, Economics and Finance, Department of Law

*Luis Jakobi*

Research assistant at the chair of Professor Dr. Liane Wörner, LL.M. (UW-Madison), University of Konstanz, Germany

## Le futur rôle des Cellules de Renseignement Financier

Kris Meskens and Julie Vanstappen

In June 2024, the EU Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) package came into effect. This package comprises one Directive and two Regulations that aim to harmonise and further strengthen the prevention of and fight against money laundering and terrorist financing in the European Union. This article describes the legislative choices and directions from the perspective of the Belgian Financial Intelligence Unit (FIU). The authors discuss how the new measures will impact the reporting of suspicious activities and transactions, enhance the analytical capacities of FIUs and facilitate the exchange of information with other competent authorities.

While not claiming to be exhaustive, the article highlights aspects that directly affect the day-to-day operations of the Belgian FIU. It pays particular attention to the organisation and independence of the FIU, cash transactions, direct access to financial and administrative databases, and the ability to suspend financial transactions and accounts.

As the establishment of a new Anti-Money Laundering Authority (AMLA) in Frankfurt am Main is considered to be the most important innovative aspect of the EU AML/CFT Package, the article also considers the role of this new body and its potential impact on the future work of FIUs.

In conclusion, the authors believe that the new AML/CFT Directive and Regulations strike a balance between providing FIUs with effective tools to combat the criminal economy and protecting the rights/concerns of individuals and companies. Through flexibility, coordination, and commitment, the EU AML/CFT package will enable FIUs to play a positive role in combatting money laundering and the financing of terrorism in the years to come.

### I. Introduction

Le 19 juin 2024, trois actes législatifs composant le nouveau paquet européen de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), en anglais « the EU AML/CTF Package » ont été publiés au Journal officiel de l'Union européenne. Ce nouveau paquet législatif, visant à renforcer le cadre de l'Union en la matière et à combler les failles favorables aux fraudeurs, comprend :

- un règlement contenant l'ensemble des obligations pour les entités assujetties en vue d'obtenir une application uniforme des règles<sup>1</sup> ;
- une sixième directive LBC/FT destinée à améliorer les systèmes nationaux de lutte contre le blanchiment de capitaux et le financement du terrorisme<sup>2</sup> ;
- et un règlement mettant en place une nouvelle autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme (ALBC)<sup>3</sup>, qui sera basée



à Francfort-sur-le-Main et débutera ses activités à la mi-2025.

Depuis le début des années 1990, les institutions européennes se sont montrées novatrices et impliquées dans la lutte contre le blanchiment de capitaux et le financement du terrorisme et l'adoption de ces trois instruments est une nouvelle étape marquante. Ce nouveau corpus législatif présente des évolutions, voire même des révolutions dans certains domaines, qui méritent notre attention. Ayant fait partie de la délégation belge responsable des négociations en ce qui concerne les aspects « Cellule de Renseignement Financier » (CRF) menant à l'adoption des instruments légaux précités<sup>4</sup>, nous tenons à parcourir avec vous ce nouveau paquet législatif du point de vue « CRF ». Notre but n'est pas d'être exhaustifs mais de mettre en lumière les aspects principaux qui touchent les CRF et influenceront la lutte anti-blanchiment et anti-financement du terrorisme dans les années à venir.

L'ensemble des actes législatifs adoptés devrait permettre d'atténuer les risques et de détecter efficacement les tentatives d'utilisation abusive du système financier de l'Union à des fins criminelles. Pour les CRF, ce cadre robuste signifie notamment : un accès plus rapide et étendu aux informations, la mise en avant de leur autonomie, de la sécurité et de la confidentialité dans l'exécution de leurs tâches, davantage d'échanges d'informations avec les autres autorités compétentes et de coopération internationale avec leurs homologues européens ainsi qu'un meilleur suivi des déclarations de soupçons.

L'expérience passée basée sur la mise en œuvre de la directive (UE) 2015/849<sup>5</sup> a mis en avant des divergences au niveau des pratiques et des approches des autorités compétentes au sein de l'Union européenne. En ce qui concerne les CRF, des rapports ont été publiés<sup>6</sup> indiquant des manquements au niveau de l'efficacité des dispositifs de coopération transfrontière afin de faire face aux nouvelles menaces de blanchiment et de financement du terrorisme. Ces dernières années, nous avons en effet assisté à une internationalisation croissante des flux financiers mais également à l'émergence et au recours à de nouvelles technologies telles que les cryptomonnaies. Sans oublier l'influence de la pandémie, qui a boosté le recours à Internet pour les achats et ventes et par conséquent le recours à de nouveaux prestataires actifs internationalement.

Disposer de structures efficaces permettant une coopération accrue des autorités compétentes sur le plan international, et notamment des CRF, est une condition sine qua non pour faire face aux risques de blanchiment et de

financement du terrorisme. Cela ne signifie pas qu'une approche globale « one size fits all » soit le meilleur choix, il fallait également tenir compte des spécificités des systèmes nationaux notamment en termes de risques et de typologies de blanchiment. Le choix et la combinaison des instruments légaux sous forme de règlements et de directives devrait garantir ce juste équilibre.

Enfin, la plus grande nouveauté du nouveau paquet LBC/FT est sans doute la création de l'ALBC, une autorité chargée de contribuer à la mise en œuvre de règles harmonisées au niveau de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Le but est de renforcer le cadre préventif en matière de LBC/FT et, plus spécifiquement pour les CRF, de renforcer les capacités d'analyse commune des déclarations de soupçons et la coopération mutuelle. L'autre pilier clé de l'ALBC est de garantir une surveillance adéquate des entités assujetties présentant des risques élevés en matière de blanchiment de capitaux et de financement du terrorisme et de promouvoir des approches communes pour la surveillance de toutes les autres entités assujetties. Les aspects de supervision européenne, impliquant la possibilité pour l'ALBC de coordonner et de contrôler des superviseurs LBC/FT du secteur financier et du secteur non-financier, y compris les organismes d'autorégulation, ainsi que de superviser directement de grands groupes financiers présents sur le marché européen, ne font pas l'objet de cet article, mais impliquent eux aussi des changements de taille. Nous ne saurions donc que trop vous conseiller de vous renseigner davantage sur ces sujets.

## II. Organisation des Cellules de Renseignement Financier

Dans la vie quotidienne, nous (les auteurs de cet article) travaillons pour la Cellule de Traitement des Informations Financières (CTIF), qui est la CRF belge. La CTIF est une autorité administrative autonome et indépendante dotée de personnalité juridique, qui correspond à la définition d'une CRF telle qu'éditée par le Groupe d'Action financière (GAFI), le Groupe Egmont des CRF et l'UE : la CRF doit être opérationnellement indépendante et autonome, chargée de recueillir et d'analyser des informations, de façon à faire le lien entre les transactions et activités suspectes et les activités criminelles sous-jacentes en vue de prévenir et de combattre le blanchiment de capitaux et le financement du terrorisme. Les termes « opérationnellement indépendante et autonome sur le plan opérationnel » signifient que chaque CRF doit être en mesure de choisir sur quelles déclarations elle travaille et quels dossiers elle disséminera à d'autres

autorités compétentes, mais aussi que chaque CRF dispose de moyens (financiers, humains...) suffisants afin de pouvoir accomplir ses tâches.

La directive (UE) 2024/1640 précise que la CRF est la cellule nationale centrale unique chargée de recevoir et d'analyser les informations qui lui sont transmises et de les disséminer à qui de droit. Il est important de souligner que malgré quelques discussions pendant les négociations du nouveau paquet LBC/FT, il n'a pas été décidé de considérer l'ALBC comme une sorte de CRF européenne chargée de recevoir les déclarations de soupçons pour ensuite les distribuer à ses acolytes CRF nationales. Ce sont les CRF nationales qui restent en charge de l'analyse des informations qui leur sont transmises en vertu de la législation LBC/FT. Il s'agit d'un choix fondamental qui explique certaines décisions (techniques notamment) au niveau des possibilités d'analyse commune et du rôle que jouera l'ALBC dans ce cadre ainsi qu'au niveau de l'architecture du système sécurisé d'échange d'informations entre CRF, le système FIU.net.

Concrètement, au sein de l'Union européenne, il existe plusieurs types de CRF : on recense des CRF administratives, policières, judiciaires ou hybrides, mais chacune a sa propre indépendance et se compose d'un organe décisionnel, d'analystes (opérationnels, stratégiques, data) et de collaborateurs administratifs, auxquels s'ajoutent des profils juridiques et IT. Le lien avec les autres autorités compétentes comme la police, les douanes ou les services de renseignement est souvent garanti par des officiers de liaison, qui peuvent être déployés au sein de la CRF ou dehors.

La directive (UE) 2024/1640 prévoit par ailleurs des exigences concernant le personnel des CRF. Les États membres devront notamment veiller à ce que ce personnel respecte des exigences professionnelles élevées en matière de confidentialité et de protection des données, et qu'il soit de la plus haute intégrité et possède les compétences nécessaires en matière de traitement responsable des ensembles de mégadonnées. Les États membres devront aussi veiller à ce que les CRF disposent de procédures pour prévenir les conflits d'intérêts.

La création de l'ALBC va notamment avoir un impact sur l'organisation des CRF dans la mesure où chaque CRF devra déléguer à l'ALBC un membre de son personnel en vue de faciliter et d'améliorer la coopération entre les CRF et l'ALBC et la réalisation d'analyses communes. Ce délégué aidera l'ALBC dans toutes les missions liées aux CRF. On pense non seulement aux analyses communes, mais aussi à la préparation des évaluations des menac-

es et des analyses stratégiques des menaces, risques et méthodes de blanchiment ou financement du terrorisme. Le délégué restera sous l'autorité de la CRF qui le délègue afin de préserver son indépendance et son autonomie sur le plan opérationnel. Tout comme le personnel de la CRF en général, il n'acceptera pas d'instructions des institutions, organes ou organismes de l'Union, des gouvernements ou d'autres organismes publics ou privés.

En ce qui concerne la structure de l'ALBC, le législateur européen a voulu mettre en place dès le départ une structure de gouvernance solide. Vu la complexité et la diversité des missions confiées à cette nouvelle autorité européenne, tant dans le domaine de la surveillance que dans celui de la coordination et du soutien des CRF, il a été convenu que les décisions ne pourraient pas être prises par un seul organe directeur. C'est pourquoi les décisions ayant trait à l'adoption d'instruments communs (telles que les normes techniques de réglementation ou d'exécution, les orientations, les recommandations...) devront être prises par le conseil général composé de représentants des autorités de surveillance ou des CRF, tandis que d'autres décisions, relatives par exemple à une entité assujettie sélectionnée ou à une autorité particulière, nécessitent un organe décisionnel plus restreint, le conseil exécutif.

En fonction de la matière traitée et afin de disposer de l'expertise nécessaire, le conseil général se réunira dans sa composition « CRF » ou dans sa composition « surveillance ». Les CRF nationales seront représentées au sein du conseil général dans sa composition « CRF » par les dirigeants des CRF (Heads of FIU) ou par un suppléant à haut niveau qui pourra remplacer le dirigeant de la CRF en cas d'empêchement de celui-ci.

Le conseil exécutif sera quant à lui composé du président de l'ALBC et de cinq membres à temps plein, dont le vice-président, nommés par le Parlement européen et le Conseil sur proposition du conseil général à partir de la liste restreinte de candidats qualifiés établie par la Commission.

### III. Entités assujetties, mesures de vigilance et déclaration de soupçons

Le cœur du travail de chaque CRF se situe dans l'analyse des déclarations de soupçons transmises par les entités assujetties au dispositif LBC/FT. Avant de s'attarder sur la déclaration en elle-même, parcourons brièvement plusieurs points sur lesquels le nouveau paquet législatif apporte des modifications et qui risquent d'avoir un impact sur l'activité déclarative.

## 1. Les nouvelles catégories d'entités assujetties

Les nouvelles technologies sont en constante évolution, offrant au secteur privé des occasions d'élaborer de nouveaux produits faisant évoluer le système financier. Loin d'être réfractaire aux innovations et au progrès, il faut néanmoins veiller à que ces développements ne créent de nouvelles failles en matière de blanchiment de capitaux et de financement du terrorisme, tant nous savons les criminels prompts à trouver les moyens d'exploiter les vulnérabilités du système pour dissimuler leurs fonds illicites<sup>7</sup>. Partant de ce constat, le règlement (UE) 2024/1624 introduit de nouvelles catégories d'entités assujetties telles que les prestataires de services sur crypto-actifs, les prestataires de services de financement participatif et les intermédiaires en financement participatif ou les clubs de football professionnel et les agents de footballeurs (qui sont d'ailleurs déjà soumis à la législation préventive en Belgique).

Par ailleurs, l'utilisation d'argent cash reste un risque majeur de blanchiment de capitaux et de financement du terrorisme<sup>8</sup>. Les divergences au niveau des régimes applicables dans les pays de l'UE ont pour conséquence que des groupes criminels peuvent encore trop facilement déplacer le profit de leurs activités criminelles entre nos pays sans passer par le circuit financier et donc sans aucun contrôle. Afin d'atténuer ces risques à l'échelle de l'Union, une limite est prévue pour les paiements en argent liquide d'un montant élevé, à savoir ceux de plus de 10 000 EUR<sup>9</sup>. Les États membres pourront néanmoins toujours choisir d'opter pour des seuils inférieurs.

En ce qui concerne l'utilisation du cash, il est également prévu dans le règlement (UE) 2024/1624 que les paiements en argent liquide et les dépôts effectués dans les locaux des établissements de crédit, d'émetteurs de monnaie électronique et de prestataires de services de paiement qui dépassent le seuil applicable au paiement en argent liquide d'un montant élevé soient déclarés à la CRF<sup>10</sup>. Ces paiements ou dépôts au-delà de la limite ne devraient néanmoins pas être considérés par défaut comme un indicateur ou un soupçon de blanchiment de capitaux, d'infractions sous-jacentes associées ou de financement du terrorisme mais la déclaration de ces transactions permet à la CRF d'évaluer et de recenser les schémas concernant les mouvements de trésorerie<sup>11</sup>.

Compte tenu de ces différentes mesures, le législateur européen a choisi de ne pas soumettre les personnes négociant des biens en général aux obligations en matière de LBC/FT. Des exceptions sont néanmoins de mise pour les personnes négociant des métaux précieux, des pierres

précieuses, d'autres biens de grande valeur et des biens culturels vu l'attrait continu et non négligeable que suscitent ces biens auprès des blanchisseurs.

Dans le paquet législatif, le législateur européen a donc conclu que les véhicules à moteur, les bateaux et les aéronefs des segments les plus élevés du marché sont vulnérables aux risques d'utilisation abusive à des fins de blanchiment de capitaux et de financement du terrorisme. Ces produits ont en effet une valeur conséquente et sont facilement transportables, deux éléments clefs recherchés par les blanchisseurs. Les personnes négociant ces biens seront donc soumises aux exigences en matière de LBC/FT<sup>12</sup>. Afin d'atténuer les risques susmentionnés et de garantir la visibilité de la propriété de ces biens, les personnes négociant des biens de grande valeur vont devoir déclarer aux CRF les transactions concernant la vente de véhicules à moteur, de bateaux et d'aéronefs lorsqu'elles atteignent un certain seuil et que ces biens sont acquis à des fins non commerciales<sup>13</sup>. Ceci vaut aussi pour les établissements financiers qui fournissent des services essentiels à la conclusion de la vente de ces biens. Ces déclarations fondées sur des seuils devront être considérées comme une communication d'information aux CRF, pas comme une déclaration de soupçons et suivront donc un autre régime au sein de la CRF. En l'état actuel des réflexions, il est prévu d'utiliser ces informations au sein de la CTIF comme une source consultable, avec laquelle chaque autre déclaration entrante pourra être comparée et qui permettra d'alimenter d'autres informations reçues.

## 2. La vigilance à l'égard de la clientèle

Les obligations de vigilance à l'égard de la clientèle que l'on retrouve dans le règlement (UE) 2024/1624<sup>14</sup> sont essentielles afin que les entités assujetties identifient, vérifient et contrôlent leurs relations d'affaires avec leurs clients, par rapport aux risques de blanchiment de capitaux et de financement du terrorisme qu'elles posent.

Une attention particulière est par ailleurs portée aux bénéficiaires effectifs, que ce soit ici dans le cadre des obligations de vigilance ou, comme nous le verrons plus tard, dans le cadre de la mise en place des registres de bénéficiaires effectifs.

En ce qui concerne la surveillance continue de la relation d'affaire et des transactions effectuées par le client, le législateur européen rappelle que les entités assujetties devraient réexaminer régulièrement les informations obtenues auprès de leurs clients, conformément à l'approche fondée sur les risques et ce, afin de conserver une

compréhension globale du profil de risque du client et de procéder à un examen approfondi des transactions.

Comme cela était déjà le cas auparavant, les entités assujetties doivent également mettre en place un système de surveillance permettant de détecter les transactions qui peuvent éveiller des soupçons de blanchiment de capitaux et de financement du terrorisme. Pour veiller à l'efficacité de la surveillance des transactions, les activités de vigilance des entités assujetties devraient en principe couvrir tous les services et produits proposés aux clients et toutes les transactions effectuées pour le compte du client ou proposées au client par l'entité assujettie. Cependant, toutes les transactions ne nécessitent pas d'être examinées séparément. L'intensité de la surveillance devrait suivre l'approche fondée sur les risques et reposer sur des critères précis et pertinents, tenant compte notamment des caractéristiques du client et du niveau de risque qui leur est associé, des produits et services proposés ainsi que des pays ou des zones géographiques concernées. Notons que l'ALBC sera chargée d'élaborer des orientations pour veiller à ce que l'intensité de la surveillance des relations d'affaires et des transactions soit adaptée et proportionnée au niveau de risque et ce, pour le 10 juillet 2026 au plus tard.

Le législateur européen a par ailleurs prévu que des mesures de vigilance renforcée devaient s'appliquer dans des cas engendrant un risque plus élevé afin de gérer et d'atténuer le risque de manière adéquate. Nous citons à titre exemplatif les relations transfrontières de correspondant ou les relations nouées avec des personnes exerçant ou ayant exercé des fonctions publiques importantes. La fourniture de services de gestion d'actifs personnalisés à des personnes présentant un patrimoine élevé pourrait également exposer à des risques spécifiques, ce qui explique que le législateur européen ait prévu un ensemble de mesures de vigilance renforcées qui devraient être appliquées au minimum, lorsque ces relations d'affaires sont réputées présenter un risque élevé de blanchiment de capitaux, d'infractions sous-jacentes ou de financement du terrorisme. Des négociations difficiles ont fini par conclure qu'un patrimoine élevé est défini comme la détention des actifs d'une valeur d'au moins 50 000 000 EUR, ou l'équivalent en monnaie nationale ou étrangère.

### 3. La déclaration de soupçons

Les entités assujetties n'ont pas seulement l'obligation d'être vigilantes à l'égard de leurs clients et des transactions effectuées, elles doivent également transmettre une déclaration de soupçons à la CRF nationale si des fonds ou activités suspectes se présentent. Tout comme les obligations

de vigilance, le volet concernant la déclaration de soupçon est désormais repris dans le règlement (UE) 2024/1624<sup>15</sup>.

Les entités assujetties devront ainsi signaler à la CRF les transactions suspectes, mais également les tentatives de transactions suspectes et les autres informations utiles pour lutter contre le blanchiment de capitaux, les infractions sous-jacentes associées et le financement du terrorisme. Ces transactions ou tentatives de transactions suspectes devront être déclarées quel qu'en soit le montant, et les références à des soupçons devraient être interprétées comme englobant les transactions, activités, comportements et schémas de transaction suspects<sup>16</sup>. Les déclarations pourraient aussi comprendre des informations fondées sur des seuils<sup>17</sup>.

Comme nous l'avons vu plus haut, la CRF fera ainsi office de cellule nationale centrale unique pour la réception et l'analyse des soupçons signalés et la dissémination des résultats de ses analyses aux autorités compétentes<sup>18</sup>.

Afin d'aider les entités assujetties à détecter des soupçons, l'ALBC sera chargée d'émettre des orientations sur les indicateurs d'activité ou de comportement suspect pour le 10 juillet 2027 au plus tard<sup>19</sup>. Compte tenu de l'évolution de l'environnement des risques, ces orientations devraient être réexaminées régulièrement et ne devraient pas préjuger de la publication par les CRF d'orientations ou d'indicateurs sur les risques et méthodes recensés au niveau national en matière de blanchiment de capitaux et de financement du terrorisme.

Parallèlement à ce qui était prévu dans les directives LBC/FT précédentes, la communication d'informations de bonne foi à la CRF par une entité assujettie, par un membre du personnel ou par un dirigeant d'une telle entité ne constituera pas une violation d'une quelconque restriction à la divulgation d'informations et ne devrait entraîner pour l'entité assujettie, ses dirigeants ou son personnel aucune responsabilité d'aucune sorte<sup>20</sup>.

Novateur en revanche est l'ajout selon lequel les entités assujetties devraient pouvoir transmettre une déclaration lorsqu'elles savent ou soupçonnent que des fonds ont été ou seront utilisés pour mener des activités criminelles, telles que l'achat de biens illicites, même si les informations dont elles disposent n'indiquent pas que les fonds utilisés proviennent de sources illicites<sup>21</sup>.

Afin de faciliter la coopération entre les CRF, déjà qualifiée de rapide et efficace, l'ALBC devra élaborer des projets de normes techniques d'exécution précisant un modèle com-



mun pour la déclaration de transactions suspectes et pour la fourniture aux CRF, par les établissements de crédit et les établissements financiers, de relevés de transactions, à utiliser comme une base uniforme dans l'ensemble de l'Union<sup>22</sup>. Ceci facilitera l'échange ultérieur de ces documents entre les CRF.

En ce qui concerne le moment auquel les entités assujetties doivent procéder à une déclaration de soupçons, le principe reste toujours d'effectuer la déclaration de soupçons avant d'effectuer la transaction. Le paquet législatif européen prévoit que les entités assujetties pourront exécuter la transaction concernée après avoir évalué les risques que présente l'exécution de la transaction si elles n'ont pas reçu d'instructions contraires de la CRF dans un délai de trois jours ouvrables à compter de la présentation de la déclaration. Nous soulignons qu'il leur sera toujours exceptionnellement possible d'exécuter une transaction suspecte avant d'en informer la CRF, lorsqu'il n'est pas possible de s'abstenir d'exécuter cette transaction ou lorsque cette abstention est susceptible d'entraver les efforts déployés pour poursuivre les bénéficiaires d'une telle transaction. Cependant, cette exception ne devrait pas être invoquée en lien avec des transactions concernées par les obligations internationales acceptées par l'État membre de la CRF visant à geler immédiatement les fonds ou autres avoirs des terroristes, des organisations terroristes ou des organisations qui financent le terrorisme, conformément aux résolutions pertinentes du Conseil de sécurité<sup>23</sup>.

#### IV. Analyse

Si l'on veut renforcer la lutte préventive contre le blanchiment de capitaux et le financement du terrorisme, il ne suffit pas d'harmoniser les règles de vigilance applicables par les entités assujetties ou d'augmenter le nombre de déclarations de soupçons transmises aux CRF. Augmenter purement et simplement le stock de déclarations auprès des différentes CRF ne devrait jamais être un but en soi, ayant notamment égard aux principes de protection de la vie privée et de « need to know » qui conditionne l'accès aux informations. Les déclarations sont effectuées suite à l'émergence de soupçons de blanchiment ou de financement du terrorisme, que ce soit sur base d'une appréciation subjective des entités assujetties ou par application de règles objectives définies par les législateurs nationaux ou internationaux (en ce qui concerne les déclarations cash par exemple).

De l'expérience de la CTIF, la tendance actuelle montre que de plus en plus d'entités assujetties, en ce compris dans les

systèmes subjectifs, commencent à recourir à l'intelligence artificielle en vue d'exécuter leur obligation de déclaration de soupçons. Tant les autorités de contrôle nationales que l'ALBC seront donc confrontées à cette évolution dans les années à venir et il conviendra de trouver un juste équilibre entre le recours à ces logiciels intelligents pour l'exécution des tâches et obligations de LBC/FT, la garantie de la qualité du contenu des déclarations de soupçons et le respect des règles de protection de la vie privée.

Au-delà du fait de veiller à la qualité des déclarations initiales, il convient de donner aux CRF la possibilité d'enrichir les informations reçues initialement avec des autres informations pertinentes provenant d'autorités compétentes ou de partenaires privés. Parcourons dès lors plusieurs mesures du nouveau paquet législatif LBC/FT que nous considérons comme des progrès pour les CRF en termes de capacité d'analyse. En dotant les CRF européennes de capacités de recherche et de transmission étendues, l'UE se présente une fois de plus comme un précurseur dans la lutte contre le blanchiment de capitaux et le financement du terrorisme.

#### 1. Les registres centraux des bénéficiaires effectifs

Attardons-nous tout d'abord sur les registres centraux d'informations sur les bénéficiaires effectifs, considérés comme essentiels pour lutter contre le détournement d'entités juridiques et de constructions juridiques à des fins de blanchiment ou de financement du terrorisme. Afin de garantir que ces registres centraux soient facilement accessibles et contiennent des données de qualité, la directive (UE) 2024/1640<sup>24</sup> instaure des règles cohérentes concernant la collecte et le stockage par les registres de ces informations. Il importe également que les États membres confient aux entités chargées des registres centraux des pouvoirs et ressources suffisants pour effectuer des vérifications concernant les bénéficiaires effectifs et s'assurer de la véracité des informations qui leur sont fournies, et pour signaler tout soupçon à leur CRF.

Aux fins de prévention et de détection du blanchiment de capitaux, de ses infractions sous-jacentes ou du financement du terrorisme, ainsi que des enquêtes et des poursuites en la matière, le législateur européen a prévu que les CRF, les autres autorités compétentes et les organismes d'autorégulation aient un accès immédiat, sans filtre, direct et libre aux informations sur les bénéficiaires effectifs.

Nous estimons que ces nouvelles mesures vont permettre d'accroître et d'unifier davantage la transparence des entreprises de l'UE, de sorte qu'il sera de plus en plus difficile

pour les criminels de se cacher derrière des entreprises et des structures juridiques européennes.

## 2. Informations sur les comptes bancaires

En vue de détecter des transferts de fonds liés au blanchiment de capitaux ou au financement du terrorisme, la directive (UE) 2024/1640<sup>25</sup> prévoit que les CRF et d'autres autorités compétentes aient rapidement accès aux informations sur l'identité des titulaires de comptes bancaires et de comptes de paiement (y compris d'IBAN virtuels), de comptes de titres, de comptes de crypto-actifs ainsi que de coffres-forts. Pour ce faire, la mise en place de mécanismes centralisés automatisés tels qu'un registre ou un système de recherche de données dans tous les États membres est dès lors primordiale.

A noter qu'afin de protéger les analyses en cours, une confidentialité complète devrait être assurée en ce qui concerne les enquêtes et demandes d'informations y afférentes émanant des CRF, de l'ALBC dans le cadre d'analyses communes et des autorités de surveillance.

Une interconnexion des mécanismes automatisés centralisés des États membres est par ailleurs prévue, pour permettre aux CRF nationales d'obtenir rapidement des informations transfrontières sur l'identité des titulaires de comptes dans d'autres États membres et renforcer leur capacité à effectuer efficacement des analyses financières et à coopérer avec leurs homologues d'autres États membres. La directive (UE) 2024/1640 prévoit que le système d'interconnexion des registres des comptes bancaire soit mis au point et géré par la Commission. Cette dernière devra assurer cette interconnexion en coopération avec les États membres, au plus tard le 10 juillet 2029.

Il est essentiel pour les CRF de pouvoir détecter rapidement les fonds illicites et les flux criminels pour pouvoir récupérer ultérieurement l'argent blanchi. Pour la CTIF-CFI, ce registre bancaire est devenu un mécanisme de recherche bien ancré au quotidien. L'interconnexion des mécanismes renforcera davantage la capacité d'analyse, mais les CRF devront néanmoins encore adapter leurs méthodes de travail afin de veiller à informer correctement la CRF du pays où le compte recherché est détenu.

## 3. Point d'accès unique aux informations concernant les biens immobiliers

Dans un même objectif de bon déroulement des analyses et des enquêtes sur des affaires criminelles potentielles, le législateur européen a par ailleurs prévu dans la directive

(UE) 2024/1640 un accès immédiat et direct des CRF et autres autorités compétentes aux informations permettant l'identification de tout bien immobilier et des personnes physiques ou entités propriétaires de ce bien, ainsi qu'aux informations permettant l'identification et l'analyse des transactions immobilières. Pour faciliter un accès effectif à ces informations, elles devront être fournies gratuitement par l'intermédiaire d'un point d'accès unique, par des moyens numériques et, si possible, dans un format lisible par machine.

## 4. L'accès des CRF aux différentes informations

De manière plus générale, les pouvoirs des CRF incluent le droit d'accéder directement ou indirectement aux informations « financières », « administratives » et « en matière répressive » dont elles ont besoin pour combattre le blanchiment de capitaux, ses infractions sous-jacentes et le financement du terrorisme. La directive (UE) 2024/1640<sup>26</sup> prévoit un accès immédiat et direct aux informations « financières » et « administratives » et un accès direct ou indirect aux informations « d'ordre répressif ».

L'accès sera réputé être un accès direct et immédiat lorsque les informations sont contenues dans une base de données, un registre ou un système électronique de recherche de données permettant à la CRF de les obtenir directement, au moyen d'un mécanisme automatisé, sans l'intervention d'un intermédiaire. Lorsque ces informations sont détenues par une autre autorité ou entité, l'accès direct suppose que les informations soient fournies à la CRF dans les plus brefs délais et sans qu'elles n'aient été filtrées par l'entité fournissant la réponse.

En ce qui concerne les informations d'ordre répressif, les États membres devront veiller à ce que la CRF se voie accorder, dans la mesure du possible, un accès direct. Si la CRF obtient un accès indirect aux informations, l'entité ou l'autorité détenant les informations devra les fournir en temps utile. Les États membres pourront autoriser la restriction de l'accès aux informations en matière répressive, au cas par cas, lorsque la transmission de ces informations est susceptible de compromettre une enquête en cours.

Jusqu'à présent, les types d'informations contenues dans les trois catégories n'étaient pas définis, ce qui impliquait une diversité au niveau des informations auxquelles les CRF de l'Union avaient accès et impactait leur capacité de coopération avec leurs homologues. Le législateur européen a donc désormais défini les ensembles minimaux d'informations « financières », « administratives » et « en matière répressive » qui devraient être mises directement

ou indirectement à la disposition de chaque CRF dans l'ensemble de l'Union.

Sans entrer dans le détail de l'ensemble des informations listées, nous noterons que les informations « financières » renvoient notamment aux informations contenues dans les registres centraux sur les comptes bancaires ainsi que les informations des entités assujetties. Les informations « administratives » comprennent quant à elles les données fiscales, les informations sur les procédures de passation de marchés publics, les données douanières, les informations figurant dans les registres nationaux de citoyenneté et de population, de sécurité sociale, des armes, des bénéficiaires effectifs ou encore dans les bases de données commerciales ou sur les voyages transfrontières. Les informations « d'ordre répressif » incluent des casiers judiciaires, des informations sur des enquêtes, des informations sur le gel ou la saisie d'avoirs ou d'autres mesures d'enquête ou mesures conservatoires, et des informations sur des condamnations et des confiscations.

#### 5. Suspension ou refus d'exécution d'une transaction et suspension de l'utilisation d'un compte ou d'une relation d'affaire

Pour des raisons d'urgence et afin d'éviter que l'argent illicite ne s'échappe et que le criminel en tire profit, les CRF doivent aussi avoir la capacité de bloquer des transactions et des fonds. Une grande majorité des CRF est d'ores et déjà habilitée à prendre ce type de mesures urgentes en vue de réaliser des analyses, de confirmer les soupçons et de disséminer les résultats des activités d'analyse aux autorités compétentes. La durée des pouvoirs en matière de suspension varie toutefois d'un État membre à l'autre, ce qui a une incidence non seulement sur le report d'activités présentant un caractère transfrontière dans le cadre de la coopération entre CRF, mais aussi sur les droits fondamentaux des particuliers.

Tenant compte de l'incidence d'une suspension sur le droit de propriété, les CRF devraient pouvoir suspendre des transactions, des comptes ou des relations d'affaires pendant une période limitée afin de préserver les fonds, de procéder aux analyses nécessaires et de diffuser les résultats des analyses auprès des autorités compétentes en vue de l'adoption éventuelle de mesures appropriées. Il reviendra aux États membres de déterminer la durée de la suspension applicable au niveau national. La directive (UE) 2024/1640<sup>27</sup> précise néanmoins que la suspension ou le refus d'exécution d'une transaction imposé par une CRF ne pourra pas dépasser dix jours ouvrables. Compte tenu de son incidence plus grande sur les droits fondamentaux de

la personne concernée, la suspension d'un compte ou d'une relation d'affaires devrait être imposée pour une période plus limitée, qui ne dépassera quant à elle pas cinq jours ouvrables.

Il sera possible pour les États membres de définir une période de suspension plus longue lorsque, conformément au droit national, la CRF exerce des compétences dans le domaine du recouvrement des avoirs ainsi que des fonctions de dépistage, de saisie, de gel ou de confiscation des avoirs d'origine criminelle. Lorsqu'une période de suspension plus longue est définie, les personnes concernées dont les transactions, comptes ou relations d'affaires ont été suspendus devraient par ailleurs avoir la possibilité de contester l'ordonnance de suspension devant une juridiction.

Nous estimons qu'à l'avenir, les CRF mettront encore plus l'accent sur la possibilité de récupérer les fonds illégaux, ce qui fait de cet article l'un des plus importants du nouveau paquet. Nous pensons que le législateur est parvenu à trouver un juste équilibre entre l'octroi de moyens suffisants aux CRF pour lutter efficacement contre la criminalité et le droit pour toute personne de disposer de ses fonds et d'être informé de manière adéquate.

#### 6. Suivi des transactions ou des activités (monitoring) et signalements après des entités assujetties

Un suivi plus étroit d'un compte ou d'une relation d'affaires peut fournir à la CRF des informations supplémentaires sur les types de transactions effectués par le titulaire du compte et conduire à la détection rapide de transactions ou activités inhabituelles ou suspectes susceptibles de justifier une nouvelle action de la CRF, y compris la suspension telle que décrite ci-dessus, l'analyse des éléments de renseignement recueillis et leur diffusion auprès des autorités chargées des enquêtes et des poursuites.

La directive (UE) 2024/1640 prévoit dès lors que les CRF soient habilitées à donner instruction aux entités assujetties de suivre, pendant une période déterminée, les transactions ou activités effectuées via un compte ou d'autres relations d'affaires gérées par l'entité assujettie. Les CRF pourront également donner instruction à l'entité assujettie de communiquer les résultats de ce suivi.

En vue d'aider les entités assujetties à étayer leurs procédures de vigilance à l'égard de la clientèle et à garantir leur cohérence avec les risques, à mettre à jour leurs systèmes d'évaluation et de gestion des risques en conséquence et à leur fournir des informations supplémentaires susceptibles d'appeler une vigilance accrue à l'égard de certains clients,

la directive (UE) 2024/1640 prévoit que les États membres veillent à ce que les CRF soient en mesure de signaler aux entités assujetties des informations pertinentes pour l'exécution des mesures de vigilance à l'égard de la clientèle. Ces signalements pourront porter sur des types de transactions ou activités, des personnes spécifiques ou encore des zones géographiques présentant des risques plus élevés. La durée d'une telle mesure devra être définie en droit national mais ne pourra pas dépasser six mois.

## 7. Analyses communes

Vu le caractère transnational du blanchiment de capitaux et du financement du terrorisme ainsi que la fréquence et l'importance des affaires transfrontières, il était également important pour le législateur européen de se pencher sur les possibilités d'amélioration de la coopération internationale entre les CRF. Afin de pouvoir aller au-delà du simple échange entre CRF, il est désormais prévu que les CRF puissent mener conjointement à bien l'activité d'analyse proprement dite et mettre en place et rejoindre des équipes communes d'analyse à des fins spécifiques et pour une durée limitée, avec l'aide de l'ALBC. Les dispositions concernant les analyses communes et le rôle de soutien que sera amenée à jouer l'ALBC dans ce cadre sont reprises tant dans la directive (UE) 2024/1640<sup>28</sup> que dans le règlement (UE) 2024/1620<sup>29</sup>. Ces mesures devraient renforcer la coopération entre les CRF et leurs connaissances mutuelles. Une vision européenne des CRF permettra d'obtenir des résultats plus transnationaux, mais exigera en même temps des ajustements dans la manière d'aborder les déclarations par chaque CRF et aura un impact sur l'allocation des ressources et la détermination des priorités.

Il est prévu que l'ALBC puisse utiliser le système FIU.net afin de pouvoir recouper des informations et apporter aux CRF un soutien opérationnel dans le cadre de l'analyse commune des affaires transfrontières. FIU.net est le système décentralisé de communication et d'échange d'informations sécurisé mis en place au niveau européen pour l'échange d'informations entre les CRF des États membres. Il sera dorénavant géré et hébergé par l'ALBC, qui en assurera la maintenance et le tiendra à jour en fonction des besoins exprimés par les CRF.

Bien que la réception des déclarations de soupçons reste une matière nationale et que les CRF continuent à être le seul destinataire et propriétaire des informations reçues des entités assujetties, le législateur européen a voulu souligner l'importance de la coopération entre les CRF et des analyses communes en donnant à l'ALBC l'opportunité de lancer des analyses communes des transactions ou

activités transfrontières suspectes. Les CRF restent toutefois maîtres et gardent leur indépendance, mais devraient tout mettre en œuvre pour accepter l'invitation de l'ALBC à participer à une analyse commune. Il est prévu qu'avec le consentement exprès des CRF y participant, le personnel de l'ALBC qui facilite la réalisation de l'analyse commune devrait pouvoir accéder à toutes les données et informations nécessaires, y compris celles relatives à l'objet du dossier. Les cas imaginés dans lesquels l'ALBC demandera le lancement d'une analyse commune sont notamment des informations exposées par des lanceurs d'alerte ou des journalistes d'investigation.

L'ALBC donnera également son soutien en élaborant des projets de normes techniques d'exécution et de réglementation ainsi qu'en publiant des orientations à l'attention des CRF. Certains sujets sur lesquels l'ALBC devra se positionner ont déjà été pré-choisis par le législateur européen dans les différents textes adoptés. On mentionnera notamment le format à utiliser pour l'échange d'informations entre CRF et celui à utiliser pour la transmission des déclarations de transactions suspectes par les entités assujetties, tout comme les critères de pertinence et de sélection à prendre en considération afin de déterminer si une déclaration de transaction suspecte concerne un autre État membre et doit donc lui être transmise par la CRF qui l'a initialement reçue.

## V. Externalisation, retours et partages d'informations

Au-delà de la réception et l'analyse des déclarations de soupçons, la mission des CRF est de pouvoir transmettre et disséminer le résultat de leurs analyses (opérationnelles et stratégiques) aux autorités compétentes concernées. Plusieurs pans de ce partage d'information ont été peaufinés ou ajoutés dans le nouveau paquet législatif, donnant à la communauté européenne des CRF des moyens plus efficaces de contribuer à des résultats concrets dans la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Les autorités compétentes auxquelles les CRF doivent pouvoir disséminer des informations incluent les autorités exerçant des fonctions en matière d'enquêtes ou de poursuites ou en matière juridictionnelle, mais également d'autres autorités qui ont des rôles spécifiques liés à la lutte contre le blanchiment de capitaux, ses infractions sous-jacentes et le financement du terrorisme, auxquelles les CRF doivent pouvoir transmettre des analyses opérationnelles ou stratégiques lorsqu'elles jugent que les résultats de leurs analyses sont pertinents pour l'exercice des fonctions de ces autorités.



## 1. Confidentialité des déclarations

Un premier point important lorsque l'on se penche sur l'externalisation par les CRF d'informations aux autres autorités compétentes concerne la confidentialité des déclarations, dans un souci de protection de l'identité de leurs auteurs. Le législateur européen a désormais explicitement prévu dans la directive (UE) 2024/1640<sup>30</sup> que la source de la déclaration de soupçons ne soit pas divulguée lorsque la CRF dissémine des informations ou lorsqu'elle répond à une demande d'informations de la part des autorités compétentes. Ce principe, d'importance primordiale, ne devrait néanmoins pas empêcher les CRF de disséminer des informations pertinentes, y compris, par exemple, des informations sur des numéros IBAN et des codes BIC ou SWIFT. Avec cette règle, l'importance du rôle des entités assujetties dans le volet préventif de LBC/FT est mise en exergue en les protégeant le plus possible contre tout effet discriminatoire ou néfaste à la suite de la transmission d'un soupçon à la CRF nationale.

C'est également dans cette optique que nous comprenons les choix qui sont faits concernant les règles applicables à la protection de la vie privée et au traitement de données à caractère personnel dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme. L'accès d'une personne visée par une déclaration de soupçons aux informations la concernant nuirait en effet non seulement gravement à l'efficacité de la lutte contre le blanchiment de capitaux et le financement du terrorisme, mais mettrait également en danger l'entité assujettie qui a honoré son obligation d'effectuer une déclaration de soupçons. Cela explique dès lors que des exceptions et restrictions au droit d'accès de la personne concernée soient prévues, cette dernière pouvant uniquement demander à une autorité de surveillance visée à l'article 51 du règlement (UE) 2016/679 ou, le cas échéant, au Contrôleur européen de la protection des données de vérifier la licéité du traitement. Sans préjudice des restrictions au droit d'accès, l'autorité de surveillance pourra uniquement informer la personne concernée que toutes les vérifications nécessaires ont été effectuées et du résultat en ce qui concerne la licéité du traitement en question, sans parler de l'analyse effectuée ou en cours par la CRF.

## 2. Communication d'informations aux superviseurs et feedback aux entités assujetties

Afin de garantir une approche globale et cohérente ainsi que de renforcer l'efficacité du dispositif de LBC/FT, il est également important que les CRF et les superviseurs coopèrent et échangent des informations de manière effective. Pour aider les superviseurs à déterminer les secteurs dans

lesquels les risques sont plus élevés ou le respect des obligations plus faible, il est prévu que les CRF leur fournissent, spontanément ou sur demande, des informations relatives notamment à la qualité et à la quantité des déclarations de soupçons soumises par les entités assujetties, la qualité et la rapidité de leurs réponses aux demandes effectuées et les résultats pertinents d'analyses stratégiques. Les CRF sont également chargées de notifier aux superviseurs lorsque des informations en leur possession indiquent des violations potentielles, par les entités assujetties, des règlements (UE) 2024/1624 et (UE) 2023/1113<sup>31</sup>.

Au niveau du feedback à fournir aux entités assujetties, il est prévu que les CRF devraient fournir au moins un fois l'an un retour d'information sur la qualité et la rapidité des déclarations de soupçons, sur la description des soupçons et sur tout autre document fourni par les entités assujetties<sup>32</sup>. Lorsque cela ne compromet pas le travail d'analyse ou d'enquête, les CRF pourraient envisager de fournir un retour d'information sur l'utilisation ou les résultats des déclarations de transactions suspectes, que ce soit sur des déclarations individuelles ou sous une forme agrégée. Il n'est néanmoins pas demandé aux CRF de donner un feedback spécifique pour chaque déclaration reçue, ce qui serait impossible vu le nombre de déclarations transmises aux CRF européennes, mais plutôt de partager des informations pertinentes comme compléments d'informations à celles que les autorités de contrôle fournissent aux entités assujetties afin de mieux cibler leur travail dans le domaine LBC/FT. Entre-temps, la CTIF a déjà commencé à chercher en collaboration avec les superviseurs des formules efficaces pour fournir aux groupes de déclarants un retour d'information adapté à leurs besoins.

## 3. Partenariats en matière de partage d'informations

Les partenariats en matière de partage d'informations entre les entités assujetties et, le cas échéant, les autorités compétentes sont devenus des outils de coopération et d'échange d'informations de plus en plus importants dans certains États membres. Le règlement (UE) 2024/1624<sup>33</sup> prévoit des règles applicables à l'échange d'informations lors de la mise en place de tels partenariats, notamment en vue d'offrir des garanties solides en matière de confidentialité, de protection des données, d'utilisation des informations et de procédure pénale.

Le législateur européen souligne par exemple que les informations reçues dans le cadre d'un partenariat en matière de partage d'informations ne devraient pas à elles seules être utilisées pour tirer des conclusions sur le risque que représente le client ou la transaction ainsi que sur le sort

d'une relation d'affaire ou l'exécution d'une transaction. Nous noterons également que l'échange d'informations sur les déclarations de soupçons ne peut avoir lieu que si la CRF à laquelle la déclaration a été présentée a approuvé cette divulgation. Le fait que des informations opérationnelles et des données à caractère personnel soient échangées, sous réserve de garanties strictes, dans le cadre de partenariats en matière de partage d'informations ne remplace par ailleurs pas les exigences prévues dans le règlement (UE) 2024/1624 en ce qui concerne le signalement de tout soupçon à la CRF compétente. Lorsque les entités assujetties détectent des activités suspectes sur la base d'informations obtenues dans le contexte d'un partenariat, elles restent tenues de signaler ce soupçon à la CRF de l'État membre dans lequel elles sont établies.

Compte tenu du mandat de l'ALBC en matière de prévention et de détection du blanchiment de capitaux, de ses infractions sous-jacentes et du financement du terrorisme, le règlement 2024/1620 prévoit également une possibilité pour l'ALBC de mettre en place un partenariat pour l'échange d'informations afin de poursuivre cet objectif.

## VI. Conclusion

Vu les différentes évolutions mises en lumière, l'impact qu'aura le nouveau paquet législatif de lutte contre le blan-

chiment de capitaux et le financement du terrorisme sur le travail des cellules de renseignement financier (CRF) sera non négligeable. Nous aurions encore pu aborder d'autres sujets propres aux CRF tels que la désignation d'un officier préposé aux droits fondamentaux ou les possibilités de médiation et d'examen par les pairs organisés par la nouvelle autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme (ALBC) compte tenu de la robustesse du nouveau corpus législatif, tant pour les CRF que pour les autres acteurs de la lutte contre le blanchiment et le financement du terrorisme.

Nous estimons que le nouveau paquet législatif européen comporte en son sein une évolution de taille pour les différents acteurs impliqués et nous pensons que ce train de mesures innovant offrira la flexibilité nécessaire pour s'adapter aux modus operandi développés par les criminels, toujours prêts à ruser afin de contourner les mécanismes existants. Les criminels disposent en effet de moyens importants en vue de blanchir leurs capitaux d'origine illicite, et le fait qu'ils ne respectent par essence aucune règle leur permet de s'adapter facilement. Les CRF ne peuvent donc compter que sur un champ d'action et un cadre réglementaire forts, deux préalables que leur offre selon nous le corpus législatif récemment adopté. Travaillant activement quotidiennement au sein d'une CRF, nous regardons dès lors vers l'avenir avec optimisme afin de contrer les procédés mis en place par les criminels.

1 Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, JO L du 19/06/2024.

2 Directive (UE) 2024/1640 du Parlement européen et du Conseil du 31 mai 2024 relative aux mécanismes à mettre en place par les États membres pour prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant la directive (UE) 2019/1937, et modifiant et abrogeant la directive (UE) 2015/849, JO L du 19/06/2024.

3 Règlement (UE) 2024/1624 du Parlement Européen et du Conseil du 31 mai 2024 instituant l'Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme et modifiant les règlements (UE) no 1093/2010, (UE) no 1094/2010 et (UE) no 1095/2010, JO L du 19/06/2024. Ce règlement est applicable à partir du 01/07/2025.

4 Du 1er janvier au 30 juin 2024, la Belgique a en effet assuré la présidence tournante du Conseil de l'Union européenne, couvrant une période à cheval entre deux législatures. Des représentants de la CTIF ont dans ce cadre participé aux trilogues précédant l'adoption des textes.

5 Directive (UE) 2024/1640 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) no 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la

Commission, JO L 141/73 du 05/06/2015.

6 Voir notamment le rapport de la Commission au Parlement européen et au Conseil portant évaluation du cadre pour la coopération entre les cellules de renseignement financier [COM(2019) 371].

7 Considérant 7 Règlement (UE) 2024/1624.

**Kris Meskens**

Secrétaire-général de la CTIF

**Julie Vanstappen**

Analyste senior – juriste opérationnelle auprès de la CTIF

8 Voir notamment le rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des risques de blanchiment des capitaux et de financement du terrorisme pesant sur le marché intérieur et liés aux activités transfrontières [COM(2022) 554 final].

9 Article 80 Règlement (UE) 2024/1624.

10 Article 80, paragraphe 4, alinéa 2 Règlement (UE) 2024/1624.

11 Considérant 162 Règlement (UE) 2024/1624.

12 Article 3 point 3) f) Règlement (UE) 2024/1624.

13 Article 74 Règlement (UE) 2024/1624.

14 Voir Chapitre III "Vigilance à l'égard de la clientèle" du Règlement (UE) 2024/1624.

15 Voir Chapitre V "Obligations de déclaration" du Règlement (UE) 2024/1624.

16 Article 69 Règlement (UE) 2024/1624.

17 Article 74 Règlement (UE) 2024/1624.

18 Article 19 Directive (UE) 2024/1640.

19 Article 69, paragraphe 5 Règlement (UE) 2024/1624.

20 Article 72 Règlement (UE) 2024/1624.

21 Article 69, paragraphe 1, a) Règlement (UE) 2024/1624.

22 Article 69, paragraphe 3 Règlement (UE) 2024/1624.

23 Article 71 Règlement (UE) 2024/1624.

24 Voir Chapitre II, Section 1 Directive (UE) 2024/1640.

25 Voir Chapitre II, Section 2 Directive (UE) 2024/1640.

26 Article 21 Directive (EU) 2024/1640.

27 Article 24 Directive (EU) 2024/1640.

28 Article 32 Directive (EU) 2024/1640.

29 Articles 40 – 43 Règlement (EU) 2024/1620.

30 Article 36 Directive (EU) 2024/1640.

31 Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849, JO L 150 du 09/06/2023.

32 Article 28 Directive (EU) 2024/1640.

33 Article 75 Règlement (UE) 2024/1624.

# The Fight against Agri-Frauds

## Suggestions to Improve Cross-Border Cooperation

Claudia Cantisani and Laura Ricci\*

This article presents the principal results of a comparative study carried out as part of the AFRADE project. Co-funded by the EU Anti-Fraud Programme, it examined fraud in shared-management funds of the common agricultural policy (CAP). The article addresses three main areas: a) the payment mechanisms for CAP funds; b) the most recurrent fraud schemes and criminal offenses; and c) the most effective tools for information exchange activities that could optimise the reporting and detection of CAP fraud among national and supranational bodies involved in both criminal and administrative investigations. The authors highlight two key issues arising from the study: the methodological and procedural approach to the subject matter and the use of administrative instead of criminal measures.

### I. Introduction

This article presents the results of a comparative research study, which was carried out in the context of the AFRADE project co-funded by the EU Anti-Fraud Programme (EU-AFP) and the University of Pisa.<sup>1</sup> It involved Italy, Poland, Bulgaria, Slovakia, and Romania. The project aimed at providing insights to help improve analytical methods for detecting fraud and irregularities concerning funds in Europe's common agricultural policy (CAP).

AFRADE's outline followed three stages, each corresponding to a key area of investigation, namely: CAP payment mechanisms, criminal patterns, and inter-authority information exchange strategies. These topics were respectively addressed in three dedicated focus groups. The project involved five legal experts from each country: Dr.

Claudia Cantisani (IT), Prof. Celina Nowak (PL); Prof. Minko Georgiev (BU); Prof. Libor Klimek (SK); and Dr. Monica Mihaela Tudor (RO). They prepared a report on their national legal system concerning the payment mechanisms for CAP funds, the most common fraud schemes/offences, and the detection and reporting of agricultural frauds. The findings in each national report were then discussed at the project's final conference. In addition, the research team used these findings to develop common guidelines for the detection and reporting of agricultural fraud.

The study was initiated because the European legal framework sets rules for reporting irregularities and suspected frauds but lacks uniformity in risk indicator assessment.<sup>2</sup> This in turn leads to varied evaluation methods across Member States that impede cooperation between national and supranational investigative bodies.<sup>3</sup>

The fragmentation among national legal systems in detecting and reporting fraud is due, in particular, to inconsistent definitions of offenses as well as administrative irregularities across EU Member States.<sup>4</sup> It is also due to the complexity of fraudulent schemes in the CAP sector. Furthermore, data on the rates of fraud are ambiguous, as they rely on investigative authorities' capabilities in detecting not just fraud *per se* but also other linked activities, such as corruption and conflicts of interest; the detection of fraud and irregularities also often depends on transparency and efficient information exchange between authorities.<sup>5</sup> In addition, public authorities involved in the payments' mechanisms (paying agencies) often operate in opaque environments – a circumstance that reinforces the need to simplify administrative procedures.

The research project addressed these issues and suggested two key strategies:

- Enhancing inductive methodologies for fraud risk analysis, focusing on case-based strategies rather than on the legal discipline of each offence;
- Increasing the integration of IT systems, and improving data accessibility and interoperability.

Before these key strategies are explained in more detail (IV. below), the article will first describe the CAP paying system (including the role of paying agencies) and the concrete functioning of control activities (II.) and then present the broader comparative results concerning CAP fraud schemes (III.).

## II. The CAP Funding System

CAP funding is basically made up of two main segments: the European Agricultural Guarantee Fund (EAGF) and the European Fund for Rural Development (EAFRD).<sup>6</sup> Payments deriving from both funds are managed at the national level by each EU country. To protect the Union's financial interests in this sector, Member States are required to set up a management and control system for payments that complies with EU rules. Moreover, they must ensure that this system functions effectively and is able to prevent, detect, and correct irregularities. Last but not least, Member States are required to use IT systems to collect and report performance data on expenditure under the CAP strategic plans.<sup>7</sup>

### 1. National paying agencies

Accredited national paying agencies and coordinating bodies<sup>8</sup> are the public entities entrusted with ensuring

the eligibility of all fund applications and the correct execution of payments to beneficiaries of CAP funds. Since they are required to provide sufficient guarantees that a claim is authorised for payment, they must undertake sufficient checks to ensure compliance with EU rules. Moreover, they must correctly and fully record the payments and submit the requested documentation to the European Anti-Fraud Office (OLAF).<sup>9</sup>

Paying agencies allocate each specific kind of fund on the basis of different requirements, depending on the type of intervention. It is important to clarify that all direct payments are granted only to active farmers. The relevant definitions, e.g., "active farmer", "agricultural activity", "agricultural area", "eligible hectare", "young farmer", and "new farmer", are provided by each national CAP Strategic Plan<sup>10</sup> in accordance with the framework given by EU legislation.<sup>11</sup> In practice, this means that these definitions may differ among Member States.<sup>12</sup>

The application for funding is highly digitalised, which simplifies both the application process and the verification of the farmer's declarations. For area-based measures and measures implemented within the framework of CAP strategic plans, in particular, the application must be submitted using the geospatial application form provided by the competent authority.<sup>13</sup> Furthermore, the declarations must be verified through the area monitoring system (AMS).<sup>14</sup> This system is used to observe, track, and assess agricultural activities and practices on agricultural land, making use of information provided by the Sentinel satellites of the European Copernicus programme, supplemented by European Geostationary Navigation Overlay Service (EGNOS) and Galileo automatically processed data.<sup>15</sup>

### 2. Means of detection and reporting

According to Art. 72 of Regulation 2021/2116, paying agencies shall annually conduct administrative checks on aid applications and payment claims to ensure their legality and regularity.<sup>16</sup> These checks are carried out on all applications for direct payments through the Integrated Administration and Control System (IACS),<sup>17</sup> which exchanges and cross-references certified information with other databases.

On-the-spot checks are conducted on only a sample of applications. According to Regulation 2021/2116, they may be executed remotely with the use of technology.<sup>18</sup> On-the-spot checks usually involve a physical visit to the farm in order to verify the accuracy of the declarations before the full aid amount is paid.



Ex-post checks, however, apply only to those measures that require the commitments be maintained after the full amount has been paid. These checks are conducted on a sample of applications and may also include a visit to the farm.<sup>19</sup>

A key role in the context of controls of applications is played by the Land Parcel Identification System (LPIS). A geographic information system established and periodically updated by Member States on the basis of aerial or spatial orthophotos,<sup>20</sup> LPIS makes it possible to geolocalise, visualise, and spatially integrate the constituent data of the Integrated Administration and Control System (IACS) at the agricultural parcel level. In this way, it enables paying agencies to determine the land's use and maximum eligible areas under the various Union aid schemes.

### III. CAP Fraud Schemes

As far as CAP fraud schemes are concerned, the study highlighted that each EU Member State (which was part of the study) more or less incorporated three main types of fraud (outlined in the PIF Directive) in its legal system:<sup>21</sup> falsity, non-disclosure, and misapplication of funds.<sup>22</sup> These types of fraudulent conduct can be divided into the following two groups:

- Undue receipt of funds, mainly based on false declarations or falsification of documents as well as on the non-disclosure of obligatory information;
- Distorted use of funds, mainly based on the misapplication of purposes the funds were granted for.

While the first type of offence requires treacherous conduct to obtain EU funds, the second type concerns legally obtained funds that are successively used for purposes other than those they were originally planned for.

The analysis revealed the following problematic issues: First, a large number of legal provisions in some countries may be ineffective, because judges struggle with establishing the elements of crimes. This is often the case in the context of misapplication of funds. Second, national legal orders include several similar provisions, as a tendency towards overlapping exists; this causes delays in the definitive application of sanctions and leads to risks of infringing the *ne bis in idem* principle.<sup>23</sup> Third, criminal sanctions can only be imposed if there is strong evidence that the crime occurred; however, fraud often follows very complex patterns, especially in the CAP sector, that depend on several factors related to the type of funds, territory, national payment mechanisms, and eligibility conditions, all of which make proving the crime difficult.<sup>24</sup>

The study found that administrative measures, such as recovering misallocated funds or excluding beneficiaries from further payments, may offer a more efficient solution than criminal sanctions. Indeed, measures like pecuniary administrative sanctions or disciplinary actions can enable authorities to intervene in the payment process earlier and are more effective in curbing fraud. They could also better target corporate compliance strategies, as companies often play a central role in fraudulent activities.

Indeed, the study's ability to identify and develop more effective solutions for preventing CAP fraud largely depends on its focus on corporate activities and the most common fraudulent strategies employed by cross-border criminal organisations. For this reason, it also included a brief analysis of the most common criminal patterns, which can be summarized as follows.

#### Common criminal patterns

To understand the structure of fraudulent offences in the CAP sector, it is important to consider that aid requirements have a significant influence on fraud patterns. The study found, in fact, that they represent a key element in understanding the mechanisms of CAP fraud. Given the historical development of the EU's common agricultural policy, the content of the aid requirements has changed over time,<sup>25</sup> with significant impact on fraudulent strategies. For example, the latest CAP reforms relate the disbursement of funds to the accomplishment of sustainability requirements (according to the conditionality principle) instead of production rates (i.e., quantitative thresholds of agricultural production).<sup>26</sup> Making the disbursement of funds dependent on the achievement of productive results makes it more difficult to resort to fraudulent strategies, because production results, in terms of agricultural yields, are quantifiable data and more easily verifiable. But, declarations of compliance with sustainability requirements call for assessments, the control of which is increasingly problematic.

It has been shown that the most common criminal patterns related to CAP shared-management funds (i.e., funds that are implemented and managed by the European Commission and the EU Member States together) are falsification or alteration of the conditions requested for disbursement of agricultural funds (e.g., false declarations regarding the farmers' land or the farmers' personal circumstances).<sup>27</sup> For example, applicants requesting direct payments may request aid for plots of land they are not entitled to, due to false agreements, or they may artificially create conditions for receiving aid and financial

support. Indirect payments, such as rural development funds, may encourage applicants to submit false invoices or falsely declare equipment as new, even though it is not. This can involve manipulated information and misrepresentations regarding compliance with the financing conditions.<sup>28</sup> Violations and falsifications may involve eligibility criteria for receiving advance payments, submitting aid requests, or accessing support schemes. Furthermore, beneficiaries may breach procurement rules, seek reimbursement for inflated costs or non-existent transactions, or even request reimbursement for costs already covered elsewhere. Notably, this last type of fraud is common in cross-border corporate crime, often carried out by organised criminal groups that establish shell companies at the same address, each with its own bank account tied to the same financial institution.

#### IV. Proposals for Improving CAP Fraud Prevention and Detection

A first key point raised by our study is the need to shift the focus from legal harmonisation to a more practical, case-by-case strategy in order to develop more effective ways of combating agri-frauds. Legal discipline will always differ from one country to another, as each Member State is free to choose how to deal with the criminalisation obligations imposed on it to protect the EU's financial interests. Fraud patterns, however, tend to display recurrent elements.<sup>29</sup> In practice, this means that they tend to be predictable to a certain extent, which makes it possible to formulate common risk assessment criteria. Consequently, a key point in the development of effective protection of the EU's financial interests is to improve the inductive methodology used to analyse the risks of CAP fraud.<sup>30</sup> Practically, this means, for example, focusing on recurrent elements of frauds as a starting point for the development of common guidelines for fraud detection.

A second key aspect emerged is the improvement of the information exchange activity and, more generally, the use of IT tools. As our study demonstrates, the early detection of fraud depends to a large extent on the quality of the information exchange systems adopted at the national and supranational levels as well as on the timeliness with which information-exchange is implemented. Depending on the Member State, digital strategies have already proven effective domestically, especially in the case of direct payments. As illustrated above (section II.1), paying agencies use IT tools to quickly check applications for CAP funding. In addition, the use of such tools enables agencies to exchange data easily with other

administrations and public entities, allowing for smooth cross-checking. At the cross-border level, however, much remains to be done. A starting point might be to increase the use of ARACHNE, a risk scoring and data mining/enrichment tool developed by the European Commission,<sup>31</sup> and to simultaneously make it more efficient and effective. Its universal use could prove decisive for the EU-wide effective prevention end: early detection of fraud. Indeed, when several countries are involved, it is crucial to rely on a data mining tool to identify red flags when processing data from more than one EU Member State.<sup>32</sup>

At the time being, many Member States already use ARACHNE.<sup>33</sup> However, it is still perceived as the least effective detection tool, especially when compared to other approaches, such as on-the-spot checks and audits, internal fraud reporting mechanisms, and fraud risk assessments of applicants and/or beneficiaries. This perception is largely corroborated by the fact that managing authorities face difficulties in collecting data (excessive administrative burden, also related to the multiplication of IT systems), accuracy issues (high number of false positives), and legal barriers (for instance, national data protection laws).<sup>34</sup> In addition, data interoperability among ARACHNE, the Irregularity Management System (IMS), and EDES (Early Detection and Exclusion System)<sup>35</sup> as well as OLAF's and other national databases should be further developed.

To properly address these points, the introduction of a distinct EU regulation in this field seems necessary. Only a broader application of ARACHNE and a consistent increase in the available data can ensure the system's proper functioning, in turn reducing the shortcomings in the accuracy of the results. This would require a specific legal duty to make the use of ARACHNE compulsory and clear, binding rules on data interoperability among EU and national databases.<sup>36</sup> Moreover, such a regulation should also provide for the extension of the use of EDES to the area of shared management funds, as this would greatly contribute to the early exclusion of unreliable entities from accessing EU funds.<sup>37</sup> Finally, well-defined rules would also be essential to ensuring full compliance with criminal procedural guarantees and with principles governing the use of artificial intelligence.<sup>38</sup>

---

\* Claudia Cantisani was responsible for writing sections I and III, Laura Ricci for sections II and IV of this article.

1 "AFRADE" stands for "Agricultural Frauds Detection: towards a more effective risk analysis and a stronger cooperation between Member States tackling frauds in European agricultural subsidies".

**Dr. Claudia Cantisani**

Research fellow, Law Department, University of Pisa; Adjunct Professor, Law Department, University of Florence

**Dr. Laura Ricci**

Postdoctoral researcher, Law Department, University of Pisa; Visiting researcher, Institute of Criminal Sciences, University of Münster

It was submitted under the Call EUAF-2021-TRAI-04. The project was led by Professor Antonio Vallini, University of Pisa.

2 See European Court of Auditors, "The Commission's response to fraud in the Common Agricultural Policy – Time to dig deeper", Special Report 14/22 of 4 July 2022; see also: European Court of Auditors, "Fighting EU-Fraud: Action Needed", Special Report 01/2019; European Commission, "34th Annual Report on the Protection of the European Union's financial interests and the fight against fraud – 2022", COM(2023) 464 final.

3 In particular, the Anti-Fraud Coordination Services (AFCOS), regulated in Art. 12a which was inserted into OLAF Regulation 883/2013 by Art. 1(13) of Regulation (EU, Euratom) 2020/2223, OJ L 437, 28.12.2020, 49.

4 For the critical issues that arise from the lack of harmonisation at the legislative level, with special regard to criminal law, see A. De Lia, "Frode nelle sovvenzioni pubbliche: una prospettiva comparata", (2022) *AmbienteDiritto.it*, 1.

5 According to the latest annual reports of the European Public Prosecutor's Office's, the number of reported and investigated cases of fraud in Italy is particularly high ("Annual Report 2021", pp. 36–37; "Annual Report 2022", pp. 36–37; "Annual Report 2023", pp. 36–37). For statistical data on percentages of reported fraud in the CAP sector in Italy, see also Comitato per la lotta contro le frodi nei confronti dell'Unione Europea (COLAF), *Relazione Annuale 2023*, vol. I, pp. 185 ff. However, the high percentages might be due to the improvement of detection mechanisms, rather the increase in offences.

6 The two funds were instituted by Council Regulation (EC) 1290/2005 on the financing of the common agricultural policy, OJ L 209, 11.8.2005, 1; the current legal framework for EAGF and EAFRD consists of: (1) Regulation (EU) 2021/2115 of the European Parliament and of the Council of 2 December 2021 establishing rules on support for strategic plans to be drawn up by Member States under the common agricultural policy (CAP Strategic Plans) and financed by the European Agricultural Guarantee Fund (EAGF) and by the European Agricultural Fund for Rural Development (EAFRD) and repealing Regulations (EU) No 1305/2013 and (EU) No 1307/2013, OJ L 435, 6.12.2021, 1, and (2) Regulation (EU) 2021/2116 of the European Parliament and of the Council of 2 December 2021 on the financing, management and monitoring of the common agricultural policy and repealing Regulation (EU) No 1306/2013, OJ L 435, 6.12.2021, 187.

7 See Art. 59 of Regulation (EU) 2021/2116., *op. cit.* (n. 6). See also: European Commission "Common agricultural policy funds", <[https://](https://agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-funds_en)

[agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-funds\\_en](https://agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-funds_en)

8 Designated by each Member State according to the detailed criteria laid down by the European Commission. For the definition of paying agencies and coordinating bodies, see Art. 9 of Regulation 2021/2116, *op. cit.* (n. 6).

9 See further: European Commission "CAP paying agencies", <[https://agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-paying-agencies\\_en](https://agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-paying-agencies_en)>.

10 Art. 4 no. 1 of Regulation 2021/2115, *op. cit.* (n. 6).

11 See, in this context, Art. 4 no. 5 of Regulation 2021/2115, *op. cit.* (n. 6).

12 For the Italian case, see art. 3 of the Agricultural Minister Decree of 23 December 2022 n. 660087.

13 Art. 69 of Regulation (EU) 2021/2116.

14 Regulation 2021/2116 required Member States to establish the AMS; it had to be operational by 1 January 2023.

15 See further: European Commission, "CAP Area Monitoring Services", <<https://dataspace.copernicus.eu/ecosystem/services/cap-area-monitoring-services>>.

16 In accordance with Art. 59 (1) lit. a) of Regulation 2021/2116.

17 According to C. Arias Navarro, D. Vidojević, P. Zdruli, F. Yunta Mezquita, A. Jones, and P. Wojda, *Integrated Administration and Control System (IACS) implementation and LUCAS data integration feasibility in the Western Balkans*, 2024, p. 4 (<<https://data.europa.eu/doi/10.2760/300751>>): "IACS consists of a series of linked electronic databases and geographic information systems that shall be used for receiving and processing applications."

18 Art. 72, sentence 2 of Regulation 2021/2116, *op. cit.* (n. 6).

19 See, for example, Agenzia regionale per le erogazioni in agricoltura, "Controlli amministrative e in loco", <<https://agea.regione.emilia-romagna.it/settori-di-intervento/sistema-dei-controlli-1/controlli-amministrativi-e-in-loco>>.

20 Art. 68 of Regulation 2021/2116, *op. cit.* (n. 6).

21 The study was based on the notion of fraud as defined in Art. 3(2) 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, OJ L 198, 28.7.2017, 29. The study also took into account the differentiation between fraud and irregularities that are purely administrative offences and defined in Art. 1(2) of Council Regulation (EC, Euratom) No 2988/95 on the protection of the European Communities financial interests, OJ L 312, 23.12.1995, 1.

22 For a brief analysis of the Italian legal system, see G. Arduzzone, "Le frodi a danno dei Fondi Agricoli Europei tra ne bis in idem e proporzionalità", (2024), <<https://www.archiviopenale.it>>, 1. As regards the other legal systems included in the study: while the Bulgarian criminal code includes financial embezzlement, document fraud, false information, illegal disbursement, and misuse of funds, the Polish legal order did not adopt the EU notion of fraud.

23 Among several Italian references on the topic, see A. De Lia, "Le Sezioni unite sul rapporto tra truffa e malversazione. L'interpretazione come 'arma letale' per la tutela degli interessi comunitari", (2017) *Giust. Pen.*, 449; S.M. Scordia, "Sulla struttura della malversazione a danno dello Stato: la giurisprudenza fa dietrofront (ma non del tutto)", (2023), <<https://www.archiviopenale.it>>, 1.

24 See, on this, N.-C. Surubaru, "European funds in Central and Eastern Europe: drivers of change or mere funding transfers? Evaluating the impact of European aid on national and local development in Bulgaria and Romania", (2021) 22(2) *European Politics and Society*, 203–221. The context-dependent analysis is also key to understanding the figures; see on this topic F.A. Roman, M.V. Achim, and R.W. McGee, "Fraud related to EU funds – The case of Romania", (2023) *Journal of Financial Studies*, 120.

25 See F. Sotte, "La politica agricola europea Storia e analisi", (2023) *Agriregionieuropa*, 21.

26 For an overview of the latest developments in agricultural law, see L. Russo, "Il Diritto agrario fra innovazione e sostenibilità", (2023) *Riv. Dir. agr.*, 464.

27 See, for example, A. Jurma and A. A. Constantinescu, "Typologies of EU Fraud. Study by the National Anticorruption Directorate, Romania" (2021) *eu crim*, 191; D. Sabev, O. Kopečný, M. Trošok, V. Kotecký, L. Máriás, P. Učeň, A. Rizea, and A. Calistru, *Where does the EU money go? An analysis of the implementation of CAP funds in Bulgaria, the Czech Republic, Poland, Slovakia and Romania*, A Report commissioned by the Greens/EFA group in the European Parliament February 2021 (<[https://www.greens-efa.eu/files/assets/docs/eu\\_agricultural\\_funds\\_web\\_220221.pdf](https://www.greens-efa.eu/files/assets/docs/eu_agricultural_funds_web_220221.pdf)>); OLAF Supervisory Committee, Opinion No 1/2021 "OLAF's recommendations not followed by the relevant authorities", Ares(2021)993638 – 4.02.2021, January 2021 (<[https://supervisory-committee-olaf.europa.eu/system/files/2021-03/opinion\\_1\\_2021\\_-\\_recommendations\\_not\\_followed\\_-\\_nc.pdf](https://supervisory-committee-olaf.europa.eu/system/files/2021-03/opinion_1_2021_-_recommendations_not_followed_-_nc.pdf)>).

28 OLAF, "The OLAF report 2020", p. 20; Jurma and Constantinescu, *op. cit.* n. (27), 192–193.

29 See *supra*, Section III.

30 Though not linked to CAP subsidies, some interesting studies apply inductive methodology in order to cope with fraudulent strategies: see S. Ramos, J. A. Perez-Lopez, R. Abreu, and S. Nunes, "Impact of fraud in Europe: Causes and effects", (2024) *Helyion*, 1.

31 This IT tool is available to Member States free of charge – and on a voluntary basis – in the areas covered by structural funds, such as the ESF and the ERDF, see further: <[https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne\\_en?prefLang=el](https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en?prefLang=el)>.

32 J. Malan, I. Bosch Chen, M. Guasp Teschendorff, and E. Nacer, *Identifying Patterns of Fraud with EU Funds under Shared Management – Similarities and Differences between Member States*, Study

requested by the CONT Committee, January 2022, pp. 41–45.

33 In the 2014–2020 multiannual financial framework (MFF) programming period, 20 Member States already used ARACHNE and, in the current programming period, two more countries have started using the tool. The majority of managing authorities use ARACHNE in conjunction with other domestic IT tools. This is the case, for example, for the Italian platform PIAF-IT; see further <<https://www.affarieuropei.gov.it/it/attivita/lotta-alle-frodi-allue/piaf-it/>>.

34 See A. Nugent and A. Schwarcz, *Instruments and Tools at EU Level and Developed at Member State Level to Prevent and Tackle Fraud – ARACHNE*, Briefing requested by the CONT committee, October 2022, pp. 2–3.

35 For EDES, see European Commission, "Early Detection and Exclusion System (EDES)" <[https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes\\_en](https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes_en)>.

36 For the envisaged development of a single integrated and interoperable information and monitoring system, including a single data-mining and risk-scoring tool, see now Recital 29 of Regulation (EU, Euratom) 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).

37 Indeed, this could make it possible to have a database of fraud cases with details on the individuals involved and company names. See further: Nugent and Schwarcz, *op. cit.* (n. 34), pp. 3–4.

38 As set out in the new European legal framework on the matter: 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 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

# Yellow Card Legislation and Infringements of Agricultural Aid Rules

## A Case Study of a Regressive Penalty Structure

Francesco Lo Gerfo\*

This article examines the administrative penalty system under the European Union's Common Agricultural Policy (CAP) in cases of over-declarations of agricultural land. It focuses on the "yellow card" legislation that was introduced in 2016 and applicable until 2022, analysing its practical implications. This "yellow card" system introduced reduced penalties for minor infractions but capped penalties at 100% of the granted aid. This approach can be regressive, as it eliminates additional penalties for irregularities over 50%. As a result, deterrent effects are lessened for serious infractions. Next to a legal analysis of the system, the author uses mathematical analysis to show that irregularities of over 40% do not lead to increased penalties. He argues that the approach followed has encouraged abuses and concludes that the EU should refrain from readopting a sanction system like the "yellow card" in the future.



## I. Introduction: Anti-Fraud Rules in CAP Regulations

The Common Agricultural Policy (CAP) is the oldest, most established, and comprehensive of the common European policies. Therefore, substantial expertise has been built in this domain in the context of the anti-fraud framework, given that the initial CAP Regulation was enacted in 1962.<sup>1</sup> Indeed, all EU legislation on the CAP established, over decades, a comprehensive system of controls, administrative penalties, and recovery provisions, both at Community and national levels – in accordance with the principle of subsidiarity.

At the Community level, the CAP anti-fraud system has remained broadly the same over the last two decades, with some detailed changes only in the rules on the calculation of penalties in the event of over-declaration. The CAP anti-fraud system is based essentially on the distinction between **circumvention**, i.e., the situation in which the conditions for obtaining the aid are “artificially created”, and the less serious **over-declaration**, which occurs when more hectares of land than actually available are included in the single payment application.

This article focuses on the over-declaration sanctioning system, its legislative development, and a comparison between the different legal frameworks regulating it throughout the years. It first presents the main features of tackling fraud patterns in CAP spending (II) and then turns to the penalty systems for CAP fraud in cases of over-declaration, which have been in place over different periods in time and which are compared in view of the penalty calculation (III.). In another step, the penalty system is also analysed from a mathematical point of view (IV.), before conclusions on the lessons for the future are drawn (V.). Based on the analyses, the conclusion is reached that the EU should refrain from adopting a penalty system like the “yellow card” system (2016–2022) again in the future.

## II. Tackling Fraud in CAP Spending

The following section features the main provisions of Union law that tackle fraud in CAP spending.

### 1. The circumvention clause

The circumvention clause is the main anti-fraud rule in the CAP. It is laid down in the EU CAP Regulations and its essence has not changed over the years. It states that **no aid is granted** to those who “artificially create the conditions” to fulfill eligibility requirements for obtaining the aid.<sup>2</sup> It is an “open” concept and covers a wide range of possible

fraud: claimants falsely presenting themselves as farmers, holdings that are non-existent or created only to access European funds, improper claims on agricultural funds by unlicensed applicants, etc. These are (usually) severe infractions with potential criminal repercussions.

### 2. The rules on over-declaration

**Over-declaration** (“intentional over-declaration”) refers to irregularities by which a farmer declares more hectares than those actually available to him or her, without a valid right of tenure (ownership, lease, concession, etc.) on the declared land, in order to obtain a higher amount of CAP aid. The legal rules on over-declaration have also remained fairly stable over the years, providing for administrative penalties that are proportional and progressive in relation to the percentage of irregularities detected. This system of “**dissuasive and proportionate**” administrative penalties is intended to discourage intentional over-declaration.<sup>3</sup>

From 2005 (the year in which the CAP was “decoupled” from agricultural production, as we know it today) to 2022, the rules on penalties for over-declaration were governed directly by EU regulations and thus uniform in all EU Member States. This included the methods for calculating the penalty. For the 2023–2027 programming period, the approach changed: Regulations (EU) Nos 2115/2021 and 2116/2021 allowed the individual EU Member States to decide on the type and level of administrative penalties to be applied to cases of over-declaration in their national CAP strategic plans. The next section focuses on the CAP administrative penalties for over-declaration and the related mathematical calculation criteria, as set out in the EU regulations. A comparison between the two different systems that were in place in the past will illustrate the Union law concepts of deterrence and the effectiveness of the penalties themselves.

## III. Comparison between the Penalty Systems

### 1. The criteria for calculating penalties for over-declaration in the years 2005–2015

The administrative penalties for the years 2005 to 2015 were governed as follows by Art. 58 of Commission Regulation 1122/2009<sup>4</sup> and Art. 19 of Commission Delegated Regulation 640/2014<sup>5</sup>:

- Over-declaration of up to 3% of the area declared (or two hectares): no administrative penalty, considered a negligible “excess” or “excusable error”;
- Over-declaration from 3% to 20% of the area declared: a figure equal to twice that of the overstated hectares is



deducted, and the aid is recalculated from the result. In sum: payment with penalty;

- Over-declaration from 20% to 50%: no aid granted; all payments are recovered;
- Over-declaration of over 50%: all payments are recovered *and* an additional penalty equal to the amount of aid/support corresponding to the difference between the area declared and the area determined is applied.

The system in force until 2015 could be considered dissuasive, reflecting the idea of effective deterrence combined with an appropriate proportionality balance between penalty and risk. This is particularly evident in the event of significant over-declarations, i.e., declarations of over 50% of the area determined, since a full recovery of the aid payments **and** an additional penalty is applied.

## 2. The criteria for calculating the penalty for over-declaration in the years 2016–2022 (“yellow card” Regulation)

Art. 1(7) of Commission Delegated Regulation No 2016/1393 inserted Art. 19a into the Commission Delegated Regulation 640/2014 amending the administrative penalty system on over-declaration for aid applications submitted from 2016 to 2022.<sup>6</sup> The method of calculating the administrative penalties in cases of over-declaration was stipulated as follows:

- Over-declaration of up to 3% of the area declared (or two hectares): no administrative penalty, considered a negligible “excess” or “excusable error”;
- Over-declaration from 3% to 10% of the area declared *and if* this is the first infringement: the aid/support shall be calculated on the basis of the area determined, reduced by 1,5 times the difference found. If an administrative penalty is imposed, it is reduced by half (50%), but this benefit is lost if a subsequent infringement is committed (“yellow card”);
- Over-declaration from 10% to 100% of the area declared: the aid/support shall be calculated on the basis of the area determined, reduced by 1,5 times the difference found. In every case, the administrative penalty shall not exceed 100% of the amounts based on the area declared.

Compared to the rules applicable for applications taken in the period from 2005 to 2015, the introduction of Art. 19a is more advantageous to farmers for the following reasons:

- The reduction rate is “only” 1,5 times that of the overstated hectares and no longer 2 times;
- A penalty reduced by half applies in minor instances (from 3% to 10% of irregularities) committed for the first and only time (in practice, this means an increase of 0,75 times that of the overstated hectares);

- The rule of an additional penalty for irregularities of more than 50% was removed;
- A maximum capping of the penalty was set<sup>7</sup>.

The last two points raise some doubts as to whether the “proportionality and dissuasiveness” of the penalty in this “yellow card” calculation system has been retained, especially if it comes to cases of serious infringement (e.g. more than 50% of irregularities).

Indeed, thanks to the *capping* of the penalty introduced by the “yellow card” legislation, the maximum risk faced by those who have committed an irregularity of 90% or even 100% is that of having to repay what they have wrongly received. Harsher sanctions are not foreseen. Having removed the additional penalty in the event of an over-declaration of more than 50%, the penalty becomes regressive as the percentage of irregularities increases. The following case examples illustrate this assumption.

**Case 1:** In 2022, a farmer declared 50 hectares of land (area declared) and obtained a payment of €200 per hectare (in sum: €10.000) but, **in reality, he only had 35 hectares available** (determined area).

- Difference in area declared – area determined (50-35) = 15 (difference found)
- $15/50 * 100\% = 30\%$  (**percentage of irregularities**)
- Irregularity rate > 10% → penalty 1,5 times the difference found ( $15 * 1,5 = 22.5$ )
- The payment should therefore be recalculated, taking into account the area determined (35) minus the difference found (15) \* 1.5 (22.5), thus  $35 - 22.5 = 12.5$
- $12.5 * 200$  (€ per hectare) = €2,500 (corrected sum to be paid)
- €10,000 had been paid.  $€10,000 - €2,500 = €7,500$  (sum to be recovered).

**Case 2:** In 2022, a farmer declared 50 hectares of land (area declared) and obtained a payment of €200 per hectare (in sum: €10,000) but, **in reality, he only had 24 hectares available** (determined area).

- Difference in area declared – area determined (50 – 24) = 26 (difference found)
- $26/50 * 100\% = 52\%$  (**percentage of irregularities**)
- Irregularity rate > 10% → penalty 1,5 times the difference found ( $26 * 1,5 = 39$ )
- The payment should therefore be recalculated, taking into account the area determined (24) minus the difference found (26) \* 1.5 (39), thus  $24 - 39 = -15$

Negative numbers cannot be applied, because it is impossible to remove more hectares of the total determined area,

to exceed 100% of the penalty, and to apply an additional penalty for infringements > 50%.

Despite the size of the irregularity (52%), the maximum penalty applicable will therefore only be the complete rescindment of the aid granted.

Case 3: In 2022, a farmer declared 50 hectares (area declared) and obtained a payment of €200 per hectare (in sum: €10,000) but, in reality, he only had 5 hectares available (determined area).

- Difference in area declared – area determined (50 – 5) = 45 (difference found)
- $45/5 * 100\% = 90\%$  (percentage of irregularities)
- Irregularity rate > 10% → penalty 1,5 times the difference found ( $45 * 1,5 = 67,5$ )
- The payment should therefore be recalculated, taking into account the area determined (5) minus the difference found (45) \* 1.5 (67.5),  $5 - 67.5 = -62.5$

However, negative numbers cannot be applied because it is impossible to remove more hectares of the total determined area, namely to exceed 100% of the penalty and thus apply an additional penalty for infringements > 50%.

Despite the size of the irregularity (90%), the maximum penalty applicable will therefore only be the complete re-

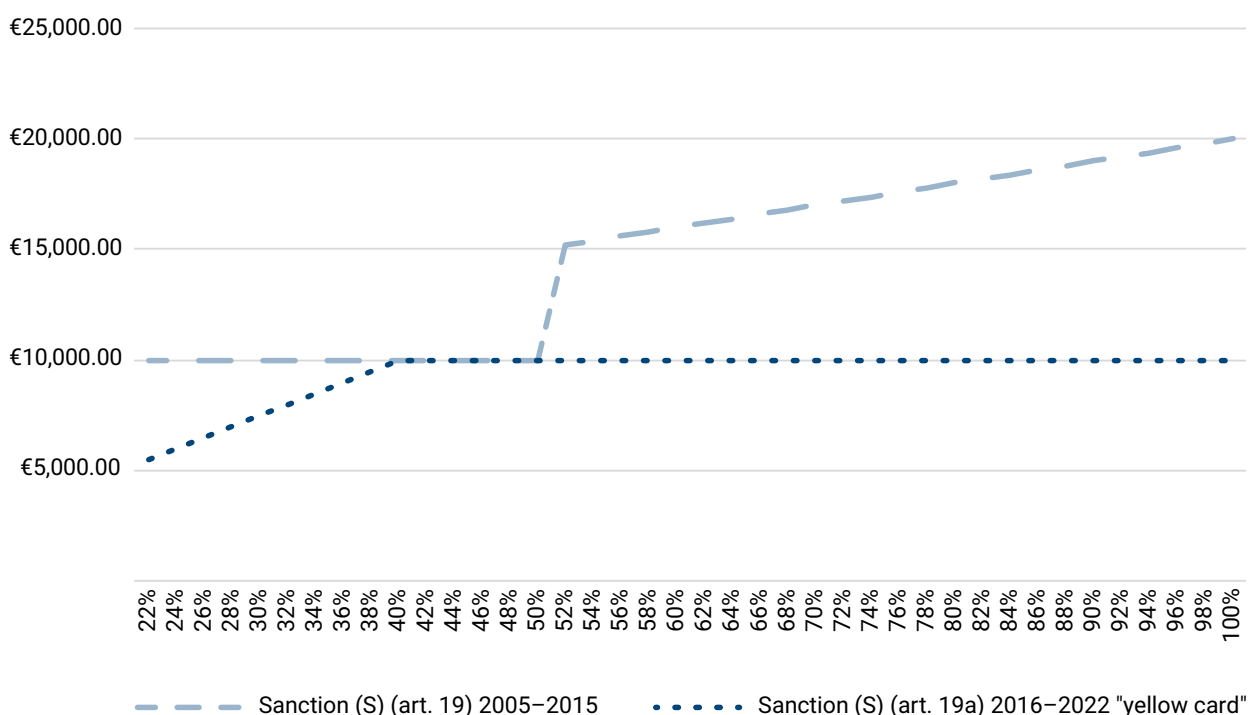
scindment of the aid granted, as in the (previous and less serious) case no 2.

### 3. Comparison between the two different sanctioning systems for over-declaration

The table on the right shows the difference between the penalty calculated under Art. 19 (for direct aid applications for the years 2005–2015) and the penalty calculated under the commonly known “yellow card” concept under Art. 19a (for direct aid applications for the years 2016–2022). The table presents various instances of *over-declaration* irregularities, ranging from 2% to 100%, taking up the above-mentioned basic case examples, i.e., area declared of 50 hectares and payment of €200/hectare (in sum: €10,000). The columns to the right show the differences in the calculation of the administrative sanctions under the two presented sanction systems in place between 2005 and 2015, on the one hand, and between 2016 and 2022, on the other.

The figure below illustrates a graphic comparison of the two sanctioning systems under Art. 19 and Art. 19a<sup>8</sup> (‘yellow card’): the ‘flattening’ of the penalty is highlighted, starting at 40% irregularity in the ‘yellow card’ system. In the other sanctioning system, however, the penalty increases with the level of irregularity, thus demonstrating greater proportionality.

#### Comparison of over-declaration sanctions under Art. 19 and Art. 19a (2005–2015 vs. 2016–2022)



## Comparison of Penalty Calculations under Art. 19 and Art. 19a (2005–2015 vs. 2016–2022)

| Payment EUR/<br>Ha | Area declared<br>(D) | Granted amount | Area<br>determined (X) | Difference Y<br>(D-X) | Irregularity | Sanction (S)<br>(art. 19)<br>2005–2015 | Sanction (S)<br>(art. 19a)<br>2016–2022<br>„yellow card“ |
|--------------------|----------------------|----------------|------------------------|-----------------------|--------------|----------------------------------------|----------------------------------------------------------|
| €200,00            | 50                   | €10.000,00     | 49                     | 1                     | 2%           | €-                                     | €-                                                       |
| €200,00            | 50                   | €10.000,00     | 48                     | 2                     | 4%           | €800,00                                | €500,00                                                  |
| €200,00            | 50                   | €10.000,00     | 47                     | 3                     | 6%           | €1.200,00                              | €750,00                                                  |
| €200,00            | 50                   | €10.000,00     | 46                     | 4                     | 8%           | €1.600,00                              | €1.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 45                     | 5                     | 10%          | €2.000,00                              | €2.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 44                     | 6                     | 12%          | €2.400,00                              | €3.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 43                     | 7                     | 14%          | €2.800,00                              | €3.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 42                     | 8                     | 16%          | €3.200,00                              | €4.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 41                     | 9                     | 18%          | €3.600,00                              | €4.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 40                     | 10                    | 20%          | €4.000,00                              | €5.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 39                     | 11                    | 22%          | €10.000,00                             | €5.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 38                     | 12                    | 24%          | €10.000,00                             | €6.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 37                     | 13                    | 26%          | €10.000,00                             | €6.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 36                     | 14                    | 28%          | €10.000,00                             | €7.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 35                     | 15                    | 30%          | €10.000,00                             | €7.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 34                     | 16                    | 32%          | €10.000,00                             | €8.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 33                     | 17                    | 34%          | €10.000,00                             | €8.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 32                     | 18                    | 36%          | €10.000,00                             | €9.000,00                                                |
| €200,00            | 50                   | €10.000,00     | 31                     | 19                    | 38%          | €10.000,00                             | €9.500,00                                                |
| €200,00            | 50                   | €10.000,00     | 30                     | 20                    | 40%          | €10.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 29                     | 21                    | 42%          | €10.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 28                     | 22                    | 44%          | €10.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 27                     | 23                    | 46%          | €10.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 26                     | 24                    | 48%          | €10.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 25                     | 25                    | 50%          | €10.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 24                     | 26                    | 52%          | €15.200,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 23                     | 27                    | 54%          | €15.400,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 22                     | 28                    | 56%          | €15.600,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 21                     | 29                    | 58%          | €15.800,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 20                     | 30                    | 60%          | €16.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 19                     | 31                    | 62%          | €16.200,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 18                     | 32                    | 64%          | €16.400,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 17                     | 33                    | 66%          | €16.600,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 16                     | 34                    | 68%          | €16.800,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 15                     | 35                    | 70%          | €17.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 14                     | 36                    | 72%          | €17.200,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 13                     | 37                    | 74%          | €17.400,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 12                     | 38                    | 76%          | €17.600,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 11                     | 39                    | 78%          | €17.800,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 10                     | 40                    | 80%          | €18.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 9                      | 41                    | 82%          | €18.200,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 8                      | 42                    | 84%          | €18.400,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 7                      | 43                    | 86%          | €18.600,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 6                      | 44                    | 88%          | €18.800,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 5                      | 45                    | 90%          | €19.000,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 4                      | 46                    | 92%          | €19.200,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 3                      | 47                    | 94%          | €19.400,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 2                      | 48                    | 96%          | €19.600,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 1                      | 49                    | 98%          | €19.800,00                             | €10.000,00                                               |
| €200,00            | 50                   | €10.000,00     | 0                      | 50                    | 100%         | €20.000,00                             | €10.000,00                                               |

#### IV. Mathematical Analysis of Penalties According to the “Yellow Card” Legislation

Art.19a of the amended Commission Delegated Regulation 640/2014 (applicable for claims from 2016 to 2022, “yellow card”) lays down the following rule:

If, in respect of a crop group [...] the area declared (D) [...] exceeds the area determined (X) [...], the aid or support shall be calculated on the basis of the area determined reduced by 1,5 times the difference found (Y) if that difference is more than either 3% of the area determined or 2 hectares.<sup>9</sup>

The administrative penalty (S) shall not exceed 100% of the amounts calculated on the basis of the area declared.

The above rule can be translated into a mathematical formula as follows:

##### 1. Definitions

D: area declared

X: area determined

Y: difference between area declared and area determined, i.e.,  $Y = D - X$

S: administrative penalty

##### 2. Formula

If  $D > X$ , the penalty (S) is calculated as:

$$S = \min \left( 1, \frac{D}{X} * X - 1.5 * Y \right)$$

whereby

$(1.5 * Y)$  is the reduction of the difference.

The penalty (S) cannot exceed 100% of the amount calculated on the area declared, so we have to take the minimum (min) between the calculated amount and 100% of the area declared.

In summary:

$$S = \min (D, X - 1.5 * Y)$$

Continuing the mathematical reasoning, we analyse the penalty formula to identify the threshold of irregularities below which the penalty remains zero, and to determine the conditions under which it vanishes.

Penalty S shall be calculated as:

$$S = \min (X - 1.5 * Y, D)$$

The penalty will be zero if the difference between the area declared and the area determined is such that the expression  $X - (1.5 * Y)$  equals zero or becomes negative. In other

words, we need to identify the situation where the difference between D and X is sufficiently small to cause the calculated penalty (according to the formula) to be zero or even negative.

To proceed, we assume:

$$X - (1.5 * Y) = 0$$

Replacing  $Y = D - X$  yields:

$$X - (1.5 * (D - X)) = 0$$

Distributing 1.5 within parenthesis yields:

$$X - (1.5 * D) + (1.5 * X) = 0$$

Combining the terms with X yields:

$$2.5 * X = 1.5 * D$$

Dividing both sides by 2,5, we obtain:

$$X = \frac{1.5}{2.5} * D$$

$$X = 0.6 * D$$

Therefore, the penalty is zero when the area determined X is 60% of the area declared D. If the area determined is 60%;<sup>10</sup> this implies an irregularity of 40% at the time of declaration. Consequently, for irregularities ranging from 40% to 100%, no penalty will be imposed; instead, only full recovery of the amount paid will apply.

#### V. Conclusions

This article compared the systems of administrative penalties for over-declarations in CAP aid applicable in the period 2005–2015 (Art. 19 of Commission Delegated Regulation 640/2014) on the one hand, and the period from 2016–2022 (Art. 19a of Commission Delegated Regulation 640/2014 as introduced by Commission Delegated Regulation 2016/1393) on the other. It illustrated that, under the new approach introduced by Art. 19a, the impact of administrative penalties has remained constant as the percentage of irregularities increases. This in turn results in a regressive penalty structure. By capping the reduction at a maximum threshold beyond which no further penalties can be imposed, and eliminating additional penalties for major infringements when irregularities exceed 50%, the regressive effect is further corroborated compared to previous rules. Case examples and mathematical calculations demonstrated that, under the legislation in force from 2016–2022, penalties do not escalate beyond an irregularity threshold of 40%. This leads to an identical treatment for

applications with 40% irregularities and those with 100%, highlighting the regressive nature of the penalty structure.

In practice, this penalty structure has offered minimal deterrence: it statistically incentivized more serious irregularities, because CAP applicants could receive higher aid while facing penalties equivalent to those for minor infractions – effectively risking only the repayment of unlawfully obtained funds, with no additional repercussions.

The results of this analysis yield a clear recommendation for the future: neither the EU nor its Member States – which regained authority over sanctioning systems for CAP irregularities in 2023<sup>11</sup> – should reinstate the “yellow card” system used for over-declarations that had been in place between 2016 and 2022. This suggests that future sanctioning systems for over-declarations must be based on a more balanced and proportionate penalty framework: a lesson from the past, to build a fairer future.

\* The views expressed in this article are exclusively those of the author and do not necessarily reflect the official opinion of the institution that employs him.

1 Regulation No 25 on the financing of the common agricultural policy, OJ 30, 20.4.1962, pp. 991–993.

2 Cf. the circumvention clauses in Art. 30 of Regulation 73/2009, OJ L 30, 31.1.2009, 16 (in force for aid applications from 2009 to 2014); Art. 60 of Regulation 1306/2013, OJ L 347, 20.12.2013, 549 (in force for aid applications from 2015 to 2022); and Art. 62 of Regulation 2021/2116, OJ L 435, 6.12.2021, 187 (in force for aid applications from 2023 to 2027).

3 See Recital 27 of Commission Delegated Regulation (EU) No 640/2014 of 11 March 2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council with regard to the integrated administration and control system and conditions for refusal or withdrawal of payments and administrative penalties applicable to direct payments, rural development support and cross compliance, OJ L 181, 20.6.2014, 48.

4 Art. 58 of Commission Regulation (EC) No 1122/2009 of 30 November 2009 laying down detailed rules for the implementation of Council Regulation (EC) No 73/2009 as regards cross-compliance, modulation and the integrated administration and control system, under the direct support schemes for farmers provided for that Regulation, as well as for the implementation of Council Regulation (EC) No 1234/2007 as regards cross-compliance under the support scheme provided for the wine sector, OJ L 316, 2.12.2009, 65, reads as follows (emphasis added by author):

“If, in respect of a crop group, the area declared for the purposes of any area-related aid schemes, except those for starch potato and seed as provided for in Sections 1 and 2 of Chapter 5 of Title IV of Regulation (EC) No 73/2009, exceeds the area determined in accordance with Article 57 of this Regulation, the aid shall be calculated on the basis of the area *determined reduced by twice the difference found if that difference is more than either 3% or two hectares, but no more than 20% of the area determined.*

If the difference is more than 20% of the area determined, no area-linked aid shall be granted for the crop group concerned.

If the difference is more than 50%, the farmer shall be excluded once again from receiving aid up to an amount equal to the amount which corresponds to the difference between the area declared and the area determined in accordance with Article 57 of this Regulation.

This amount shall be off-set from payments in accordance with Article 5b of Commission Regulation (EC) No 885/2006. If the amount

cannot be fully off-set in accordance with that article in the course of the three calendar years following the calendar year of the finding, the outstanding balance shall be cancelled.”

5 Art. 19 of Commission Delegated Regulation 640/2014, *op. cit.* (n. 3), (applicable for applications until the year 2015) reads as follows (emphasis added by author):

“1. If, in respect of a crop group as referred to in Article 17(1), the area declared for the purposes of any area-related aid schemes or support measures exceeds the area determined in accordance with Article 18, the aid shall be calculated on the basis of the area determined reduced by *twice the difference found if that difference is more than either 3% or two hectares, but no more than 20% of the area determined.*

If the difference is more than 20% of the area determined, no area-related aid or support shall be granted for the crop group concerned.

2. If the difference is more than 50%, no area-related aid or support shall be granted for the crop group concerned. Moreover, the beneficiary shall be subject to an additional penalty equal to the amount of aid or support corresponding to the difference between the area declared and the area determined in accordance with Article 18.

3. If the amount calculated in accordance with paragraphs 1 and 2 cannot be fully off-set in the course of the three calendar years following the calendar year of the finding, in accordance with the rules laid down by the Commission on the basis of Article 57(2) of Regulation (EU) No 1306/2013, the outstanding balance shall be cancelled.”

6 Art. 19a inserted by Commission Delegated Regulation (EU) 2016/1393 of 4 May 2016 amending Delegated Regulation (EU) No 640/2014 supplementing Regulation (EU) No 1306/2013 of the European Parliament and of the Council with regard to the integrated administration and control system and conditions for refusal or with-

### Francesco Lo Gerfo

Magistrate, Seconded National Expert at the European Commission, OLAF





drawal of payments and administrative penalties applicable to direct payments, rural development support and cross compliance, OJ L 225, 19.8.2016, 41, reads as follows:

“1. If, in respect of a crop group as referred to in Article 17(1), the area declared for the aid schemes provided for in Chapters 1, 2, 4 and 5 of Title III and in Title V of Regulation (EU) No 1307/2013 and the support measures referred to in Articles 30 and 31 of Regulation (EU) No 1305/2013 exceeds the area determined in accordance with Article 18 of this Regulation, the aid or support shall be calculated on the basis of the area determined reduced by 1,5 times the difference found if that difference is more than either 3% of the area determined or 2 hectares.

The administrative penalty shall not exceed 100% of the amounts based on the area declared.

2. Where no administrative penalty has been imposed on the beneficiary under paragraph 1 for over-declaration of areas for the aid scheme or support measure concerned, the administrative penalty referred to in that paragraph shall be reduced by 50% if the difference between the area declared and the area determined does not exceed 10% of the area determined.

3. Where a beneficiary had his administrative penalty reduced in accordance with paragraph 2 and another administrative penalty as referred to in this Article and in Article 21 is to be imposed on that beneficiary for the aid scheme or support measure concerned in respect of the following claim year, he shall pay the full administrative penalty in respect of that following claim year and shall pay the amount by which the administrative penalty calculated in accordance with paragraph 1 had been reduced in accordance with paragraph 2.

4. If the amount calculated in accordance with paragraphs 1, 2 and 3 cannot be fully off-set in the course of the three calendar years following the calendar year of the finding, in accordance with Article 28 of Implementing Regulation (EU) No 908/2014, the outstanding balance shall be cancelled.”

7 Art. 19a(1) subpara. 1 of the amended Commission Delegated Regulation 640/2014, *op. cit.* (n. 6).

8 In the Italian version “Art. 19 *bis*”.

9 See the wording in note 6 *supra*.

10 This is expressed by the following formula:  $X \geq 0.6 * D$ .

11 See above I.

## Non-Conviction-Based Confiscation (NCBC) – A Reform Option for German Asset Recovery Law

Fabian M. Teichmann

Cross-border, asset-related crime exploits a persistent enforcement gap in Germany’s confiscation regime. Existing tools – conviction-based forfeiture under §§ 73 ff. German Criminal Code (StGB) and the narrowly framed conviction-independent procedure of § 76a StGB – fail whenever offenders abscond, die, or hide behind complex offshore structures. This article addresses two research questions: (1) Can a non-conviction-based confiscation (NCBC) mechanism close this gap effectively? (2) Is such a mechanism compatible with the property guarantee of Art. 14 Basic Law and the fair-trial safeguards of Art. 6 European Convention on Human Rights?

Building on Directive (EU) 2024/1260 on asset recovery; comparative practice in Switzerland (SRVG 2015), Italy (*confisca di prevenzione*), and the United Kingdom (Proceeds of Crime Act 2002); and German constitutional jurisprudence, the author proposes a *Vermögenseinziehungsgesetz* (VEG, Asset Confiscation Act). The VEG is conceived as an *in rem* civil procedure before specialised chambers: the public prosecutor must demonstrate the “overwhelming probability” of illicit origin (i.e., an evidentiary standard lying between reasonable suspicion and proof beyond reasonable doubt, roughly 75% likelihood); only then does the owner assume a secondary burden to substantiate lawful provenance. Annual judicial review, hardship compensation, and a federal Asset Recovery Office would help safeguard due process. The proposal also recommends that data processing follow the principles of the General Data Protection Regulation, while cross-border enforcement interfaces with Regulation (EU) 2018/1805. The analysis demonstrates that the VEG model would satisfy Union minimum standards and the proportionality test of the German Federal Constitutional Court, thereby transforming the maxim “crime must not pay” into a legally and practically attainable objective.

### I. Introduction

Corruption, money-laundering, and organised-crime profits are moved rapidly across jurisdictions, concealed behind offshore vehicles and reinvested in opaque asset classes

such as cryptocurrencies or high-value real estate. Whenever a criminal conviction cannot be secured – because the suspect dies, absconds, remains unidentified, or enjoys home-state immunity – conviction-based confiscation under §§ 73 ff. German Criminal Code (*Strafgesetzbuch*, StGB) and

the auxiliary mechanisms of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO) reach their limits. A measurable enforcement gap arises in which illicit assets remain untouched and continue to fuel criminal markets.<sup>1</sup>

The 2017 overhaul introduced (limited) conviction-independent confiscation in § 76a StGB, yet even this procedure still hinges on (i) a specific unlawful act and (ii) at least reasonable suspicion of a criminal offence (§ 152(2) StPO). Consequently, Germany does not yet meet the minimum standard laid down in Art. 12 et seq. Directive (EU) 2024/1260, which expressly calls for genuine non-conviction-based confiscation (NCBC).<sup>2</sup> Against this background, this article will present a reform proposal for the German legislator.

The analysis employs a three-pillar approach: doctrinal analysis of current German law; comparative evaluation of Swiss, Italian, and UK confiscation models; and legal-policy assessment against Directive (EU) 2024/1260 and FATF Recommendation no 4.

The following roadmap will guide the reader through the lines of argument towards an own proposal that seeks to remedy Germany's enforcement gap in the future.

## II. Enforcement Issues under German Law

The 2017 Act on the Reform of Criminal Asset Forfeiture established three statutory avenues of confiscation in Germany: (i) conviction-dependent substantive confiscation under §§ 73 ff. StGB, (ii) extended confiscation under § 73a StGB, and (iii) a conviction-independent confiscation procedure in § 76a StGB read in conjunction with §§ 435 ff. StPO. While the reform harmonised terminology and strengthened tracing powers, each pillar remains tethered to elements that can collapse once a criminal trial is no longer feasible. Substantive and extended confiscation presuppose a final conviction, thereby excluding cases in which defendants die, abscond, or enjoy immunity. Even the supposedly independent route of § 76a StGB is conditioned on the identification of a specific unlawful act *and* at least an initial suspicion of a criminal offence pursuant to § 152(2) StPO; this means that neither a pure *in rem* approach nor proceedings against assets of unknown provenance are legally possible in Germany.

Empirical practice exposes the resulting enforcement deficit. Assets parked in multi-layered offshore structures – the “Panama Papers” typology – cannot be accessed because the beneficial owner and the predicate offence remain opaque.<sup>3</sup> The death or permanent flight of key suspects

likewise extinguishes the possibility of a conviction-based order, and politically exposed persons in non-cooperative jurisdictions often benefit from *de facto* immunity. Transparency deficits regarding beneficial ownership mean that investigations frequently stall at the straw men, while the true profiteers keep control of illicit gains, perpetuating criminogenic incentives.

Directive (EU) 2024/1260 consciously addresses these very scenarios by obliging EU Member States to introduce a genuine non-conviction-based confiscation mechanism.<sup>4</sup> Germany, however, still binds confiscation to an offence- or offender-related nexus and therefore falls short of the Directive's minimum standard. The material and procedural lacuna thus identified underscore the necessity of an autonomous *in rem* framework – one that can operate on the “overwhelming probability” of illicit origin (albeit remaining anchored in due process guarantees).

Against this backdrop, the analysis set out below turns to the international and Union law parameters shaping any German reform initiative. This analysis paves the way for a comparative evaluation of existing NCBC models and, ultimately, for the proposed *Vermögenseinziehungsgesetz* that seeks to close the enforcement gap without eroding constitutional safeguards.

## III. International and Union-Law Framework

The normative groundwork for any German non-conviction-based confiscation (NCBC) regime is laid by a concentric set of obligations that begin at the global level and culminate in binding Union law, in particular the United Nations Convention against Corruption (UNCAC).<sup>5</sup> The Financial Action Task Force (FATF) refined this UNCAC provision mandate in its 2023 best-practice note to Recommendation 4, calling for “effective NCBC instruments” that incorporate judicial control, safeguards for bona-fide third parties, and rapid international cooperation.<sup>6</sup>

Within Europe, Directive (EU) 2024/1260<sup>7</sup> constitutes the most stringent legal framework. It obliges EU Member States to establish a tiered confiscation system that includes – alongside traditional conviction-based measures (Arts. 12–14) – a genuine NCBC option for cases of illness, death, flight, or prescription of the accused (Art. 15).<sup>8</sup> It further introduces “Unexplained Wealth Orders”, empowering courts to confiscate assets grossly disproportionate to declared income if lawful origin cannot be substantiated (Art. 16), and mandates the creation of specialised asset-recovery and management authorities (Arts. 6–9).<sup>9</sup>

Complementing the Directive, Regulation (EU) 2018/1805 on mutual recognition of freezing and confiscation orders ensures that NCBC decisions will circulate seamlessly once issued.<sup>10</sup> The Regulation obliges every Member State to recognise foreign orders “without further formalities” and confines refusal grounds to narrowly drawn exceptions such as *ne bis in idem*. Consequently, any German reform must furnish courts with interfaces – standardised certificates and expedited enforcement channels – that align with this automatised recognition architecture.

Taken together, UNCAC, FATF standards, Directive (EU) 2024/1260, and Regulation (EU) 2018/1805 form a multi-layered matrix requiring compliance. They compel Germany to close its enforcement gap while leaving calibrated discretion regarding proof standards, procedural design, and asset-management structures. A newly developed law must therefore translate these external imperatives into a constitutionally coherent domestic framework that balances the effectiveness of confiscation with the property guarantee of Art. 14 Basic Law (*Grundgesetz*, GG) and the fair-trial safeguards of Art. 6 ECHR.<sup>11</sup>

#### IV. Comparative Analysis of Existing NCBC Regimes

The ensuing comparative analysis is not intended as a mere descriptive exercise. Rather, it distils the decisive design choices of three mature NCBC regimes – Switzerland, Italy, and the United Kingdom – in order to extract “lessons learnt” that inform the subsequent drafting of a German “*Vermögenseinziehungsgesetz*”. Each jurisdiction is examined with a view to (i) evidentiary thresholds, (ii) procedural safeguards, and (iii) asset-management architecture. The findings are then used as benchmarks for the VEG proposal in Part V.

The Swiss Federal Act on the Freezing and Restitution of Illicitly Acquired Assets of Foreign Politically Exposed Persons of 2015 (hereinafter: SRVG)<sup>12</sup> empowers the Federal Council (*Bundesrat*) to impose a summary freeze for an initial four-year period – extendable up to twenty years where mutual legal assistance fails – whenever a country of origin displays systemic corruption or has undergone a regime change. The core mechanism lies in Art. 15 SRVG: a sudden, inordinate increase in a politically exposed person’s assets triggers a presumption of illicit origin, shifting the burden onto the individual to rebut that presumption on the “overwhelming of probability”. While this facilitates swift intervention, Swiss scholars have voiced concern about intrusions on the constitutional property guarantee (Art. 26 *Bundesverfassung*) and potential tensions with the

presumption of innocence and reasonable time safeguards under Art. 6 ECHR.<sup>13</sup>

Italy’s *confisca di prevenzione*, introduced by the Rogno-ni-La Torre Law 646/1982 and refined through subsequent reforms, targets individuals who are suspected of belonging to a mafia type organization and individuals who, on account of their behaviour and lifestyle and on the basis of factual evidence, may be regarded as habitually living, even in part, on the proceeds of crime.<sup>14</sup> The measure is ordered by specialised *misure di prevenzione* courts in autonomous proceedings; proof may rest on a circumstantial bundle amounting to “overwhelming probability” that the assets cannot be reconciled with lawful income. The European Court of Human Rights has generally upheld this preventive model, provided that strict proportionality and full judicial review are observed.<sup>15</sup>

In the United Kingdom, Part 5 of the Proceeds of Crime Act 2002<sup>16</sup> establishes a civil recovery procedure administered by the National Crime Agency before the High Court.<sup>17</sup> The State must prove, on the ordinary “balance of probabilities”, that property represents the proceeds of unlawful conduct; no criminal conviction is required. The 2018 amendment introduced Unexplained Wealth Orders (UWOs), compelling respondents to account for assets whose value appears disproportionate to their known income and enabling interim freezing orders pending explanation. British practice records high settlement rates but also significant litigation and administrative costs, leading to calls for tighter cost-benefit controls.<sup>18</sup>

Taken together, these three jurisdictions illustrate a spectrum of NCBC techniques: Switzerland prioritises asset preservation through extended freezes and reversed burdens; Italy embeds confiscation in a preventive-justice framework focused on mafia-type/organised crime, and the UK deploys a fully civil law, asset-centred recovery model coupled with disclosure obligations. Despite divergent legal traditions, each system combines lower evidentiary thresholds with robust judicial oversight, thereby offering workable blueprints for a German *Vermögenseinziehungsgesetz* while underscoring the constitutional need for proportionality, due process, and third-party protection.

#### V. Core Elements of a *Vermögenseinziehungsgesetz* (VEG)

The following outlines a proposal for a *Vermögenseinziehungsgesetz* (VEG). While it engages with the academic model proposed by Wegner/Ladwig/Zimmermann/

*El-Ghazi*,<sup>19</sup> it departs notably from that draft in several material respects: adopting an “overwhelming probability” evidentiary standard (rather than mere plausibility), relocating the proceedings to specialised chambers of civil courts instead of criminal courts, and centralising asset management in a federal office.<sup>20</sup>

- The VEG rests on the federal annex competence for criminal law under Art. 74(1) No. 1 GG. Confiscation is framed as a repressive measure that eliminates unjust enrichment rather than a police-law intervention, meaning that the German Bundesrat’s consent is unnecessary; nevertheless, a cooperative federal-state model is envisaged to manage implementation costs.
- Proceedings are conceived as a strictly in rem civil action before a three-judge chamber following the principles of the German Code of Civil Procedure (Zivilprozessordnung, ZPO).<sup>21</sup> The public prosecutor, acting as plaintiff, must substantiate the illicit origin of the asset; only then does the owner assume a secondary burden to demonstrate lawful provenance. The chamber has an enhanced duty of clarification under § 139 ZPO, ensuring that a lowered evidentiary threshold does not jeopardise factual accuracy.
- That threshold is set at “overwhelming probability” (≈ 75%), situated between mere reasonable suspicion and full criminal proof. Once this standard is met, the owner’s cooperation duty is limited and never punitive; silence may permit – but does not compel – adverse inference.
- Interim protection relies on familiar Code of Civil Procedure (ZPO) instruments: attachments, security mortgages, and account seizures can be ordered on the same evidentiary threshold, subject to annual judicial review and a maximum duration of four plus four years (“4 + 4 model”) in order to avoid excessive durations of these measures. A three-tier appeal chain (analogous to § 567 ZPO, German Federal Court of Justice, German Federal Constitutional Court) guarantees layered oversight and compliance with the “reasonable time” requirement of Art. 6 ECHR.
- Asset management is centralised in a Federal Asset Recovery Office (ARO). Real estate vests ex lege in the federation and is first screened for interim public use by the Federal Agency for Real Estate (Bundesanstalt für Immobilienaufgaben, BImA) before public sales; crypto-assets move to a joint ARO/Deutsche Bundesbank<sup>22</sup> multi-sig wallet<sup>23</sup> with a ±20 % volatility buffer.<sup>24</sup> Net proceeds, after costs and hardship compensation, are split 50:50 between the federation and federal states (Länder), and an annual public report ensures transparency.<sup>25</sup>
- Data processing draws its legality from Art. 6 (1)(c) GDPR; where necessary for law-enforcement aims, data subject rights may be proportionately restricted under

Art. 23 GDPR. A five-year automated storage review and a two-stage judicial remedy for access requests embed purpose limitation and minimisation principles.

- Retroactivity is limited to a permissible *unechte Rückwirkung*: assets generated before 1 January 2027 fall within the scope of the VEG, but criminal liability remains unaffected. A hardship-cum-compensation clause<sup>26</sup> and the moderate proof standard prevent excessive encroachment on Art. 14 GG property guarantees while meeting EU minima criteria.

## VI. Evaluation and Outstanding Issues

Pre-legislative modelling suggests that an NCBC mechanism framed along the lines of the VEG (as proposed in Section V.) could raise Germany’s annual asset-recovery yield by up to one third, mirroring the empirical uptick observed after introduction of civil recovery in the United Kingdom and the *confisca di prevenzione* in Italy.<sup>27</sup> Yet comparative evidence also shows diminishing marginal returns once the “low-hanging fruit” of readily traceable real estate and bank deposits have been harvested; complex crypto-assets and art portfolios remain resistant to seizure, despite lowered proof standards.<sup>28</sup> Budgetary analyses by the Swiss Federal Audit Office have indicated that every Swiss franc spent on asset management under the SRVG generates roughly 4.6 francs in realised value, but only where a specialised recovery office ensures professional stewardship and rapid disposal; *ad hoc* local administration, by contrast, erodes net proceeds through storage and litigation costs.<sup>29</sup>

The German Federal Constitutional Court accepts preventive confiscation if (i) the measure pursues a weighty public interest, (ii) less intrusive alternatives are unavailable, and (iii) procedural design embeds robust judicial review.<sup>30</sup> The proposed VEG meets these criteria by tying definitive deprivation to an “overwhelming probability” threshold, by granting owners a secondary – but never punitive – burden of explanation, and by anchoring the entire procedure in the ordinary civil courts with a full appellate chain. Nevertheless, two grey zones persist.<sup>31</sup> First, the compatibility of adverse inference from silence with the *nemo tenetur* principle has not yet been conclusively tested by the German Federal Constitutional Court; second, the retroactive inclusion of assets accrued before 2027, though limited to *unechte Rückwirkung*, may provoke scrutiny under the Constitutional Court’s doctrine of legitimate expectations.<sup>32</sup>

Regulation (EU) 2018/1805 promises frictionless recognition of NCBC orders, yet practice under the predecessor Framework Decision shows persistent delays because dual

criminality is disputed or third-party rights are invoked.<sup>33</sup> The VEG therefore incorporates standardised certificates and a 15-day execution timeline, but real-world compliance depends on adequate staffing of both the Asset Recovery Office and the judicial network of contact points.

Finally, socio-economic externalities merit systematic monitoring. While confiscation curtails criminal capital flows, abrupt disposal of large real-estate portfolios can depress local property markets, and forced liquidation of shareholdings may disrupt corporate governance.<sup>34</sup> The VEG mandates an *ex-ante* macro-impact assessment for seizures exceeding €50 million and empowers the German Ministry of Finance to stagger public sales to mitigate market shock. Yet, no mechanism presently compensates communities indirectly harmed by asset freezes — an issue flagged in the FATF 2023 best-practice note but left unresolved by Directive 2024/1260.

In sum, the proposed framework is both feasible and constitutionally defensible, but its ultimate success turns on practical resourcing, judicial capacity, and continuous evaluation of collateral effects. These open issues constitute the agenda for mid-term legislative review and empirical research once the VEG has been in force for five years.

## VII. Conclusion

Germany's current confiscation architecture leaves a demonstrable enforcement gap whenever a criminal conviction is unattainable. A look at the United Kingdom's civil recovery scheme and Italy's *confisca di prevenzione* confirms that a genuine non-conviction-based confiscation instrument measurably increases asset-recovery yields without undermining due process, provided that judicial oversight and proportionality safeguards are in place. Directive (EU) 2024/1260 now obliges all Member States to adopt such an instrument, and Germany would be exposed to infringement proceedings should implementation lag.

The *Vermögenseinziehungsgesetz* (VEG) proposed here would fulfil these supranational requirements and remain within the constitutional corridor set by the German Federal Constitutional Court: it ties definitive deprivation to an "overwhelming probability" evidentiary standard, embeds a full appellate chain and annual judicial review, and tempers the evidentiary burden-shifting with a non-punitive inference rule. In this way, the VEG would respect both the right to property (Art. 14 GG) and fair trial requirements of Art. 6 ECHR, in particular the requirement to reach a court decision within reasonable time.

Legislative priority should now focus on the following:

- Enacting the VEG ahead of the Directive's transposition deadline;
- Allocating stable funding for the Federal Asset Recovery Office and its counterparts in the Länder;
- Mandating a five-year empirical review to monitor effectiveness, market impact, and constitutional practice.

By doing so, the German legislature can transform the normative maxim "crime must not pay" into a practically attainable goal, closing the enforcement gap while simultaneously upholding rule-of-law guarantees for property owners and *bona fide* third parties alike.

1 In Germany: Sections 73 et seq. of the German Criminal Code (*Strafgesetzbuch* – *StGB*), and Sections 111b et seq. of the German Code of Criminal Procedure (*Strafprozessordnung* – *StPO*). An English translation of these laws is available under: <[https://www.gesetze-im-internet.de/Teilliste\\_translations.html](https://www.gesetze-im-internet.de/Teilliste_translations.html)>. All hyperlinks in this article were last accessed on 5 July 2025.

2 Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, OJ L, 2024/1260, 2.5.2024.

3 OECD (2024), *Beneficial Ownership and Tax Transparency – Implementation and Remaining Challenges*, p.10.

4 H. Matt, "Criminal law principles should be applied in all asset recovery cases throughout the EU", (2024) 15(4) *New Journal of European Criminal Law*, 373–374.

5 , The 2004 United Nations Convention against Corruption can be retrieved here: <[https://www.unodc.org/documents/brussels/UN\\_Convention\\_Against\\_Corruption.pdf?utm\\_source=.com](https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf?utm_source=.com)>.

6 FATF (2025), *Best Practices on Confiscation Recommendations 4 and 38 and a Framework for Ongoing Work on Asset Recovery*, retrievable at <<https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>>.

7 *Op. cit.* (n. 2).

8 See also F. Meyer, "Recognizing the unknown – the new confiscation regulation", (2020) 10(2) *European Criminal Law Review*, 141–144; S. Oliveira e Silva, "Regulation (EU) 2018/1805 on the mutual recognition of freezing and confiscation orders: A headlong rush into Europe-wide harmonisation?" (2022) 13(2), *New Journal of European Criminal Law*, 202–214.

9 For the key points of the Directive, see European Union, *Proceedings in criminal matters – asset recovery and confiscation*, 2024, <[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum%3A4757305&utm\\_source=.com](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum%3A4757305&utm_source=.com)>; T. Wahl, "New Directive on Asset Recovery and Confiscation", *eu crim* 1/2024, 37–38.

10 Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14.11.2018 on the mutual recognition of freezing orders and confiscation orders, O.J. L 303, 28.11.2018, 1; C.M. King and V. Schlösser, "A 'continuous' battle against organized crime and illicit enrichment through the new proposal for a Directive for the confiscation of assets", (2024). 3 *Yearbook of International & European Criminal and Procedural Law* 517–663, 531. For a summary of the Regulation, see T. Wahl, "Regulation on Freezing and Confiscation Orders", *eu crim* 4/2018, 201–202.



- 11 See further, on the latter point, ECtHR, Decision of 5 July 2005, *Van Offeren v. Netherlands*, Appl. No. 19581/04 and the following ECtHR judgments: ECtHR, 5 July 2001, *Phillips v. United Kingdom*, Appl. no. 41087/98, § 44 and ECtHR, 23 September 2008, *Grayson and Barnham v. United Kingdom*, Appl. nos. 19955/95 and 15085/96, § 47.
- 12 Bundesgesetz über die Sperrung und die Rückerstattung unrechtmässig erworbener Vermögenswerte ausländischer politisch exponierter Personen (SRVG) vom 18. Dezember 2015, SR 196.1. The law is available in English, German, French, and Italian at: <https://www.fedlex.admin.ch/eli/cc/2016/322/de>.
- 13 P. Reich, M. Rolaz, K. Projer, S. Salsench & A. Zellweger, "Swiss Government Analysis of the EU Directives on the Recovery and Confiscation of Illicit Assets and on the Violation of Restrictive Measures", *Global Sanctions and Export Controls Blog*, 19 December 2024, <https://sanctionsnews.bakermckenzie.com/swiss-government-analysis-of-the-eu-directives-on-the-recovery-and-confiscation-of-illicit-assets-and-on-the-violation-of-restrictive-measures/>; A. Vieira, "Non-Conviction Based Confiscation and Unexplained Wealth Orders: A Contradiction in Terms?", *Fair Trials*, 26 March 2025, <https://www.fairtrials.org/articles/legal-analysis/non-conviction-based-confiscation-and-unexplained-wealth-orders-a-contradiction-in-terms/>; P. de Preux, "Switzerland: How seizure and forfeiture of Russian assets works in practice", *Global Investigations Review GIR*, 17 May 2024, <https://globalinvestigationsreview.com/review/the-european-middle-eastern-and-african-investigations-review/2024/article/switzerland-how-seizure-and-forfeiture-of-russian-assets-works-in-practice>.
- 14 Rognoni-La Torre Nr. 646/1982, available under: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1982-09-13:646#nav>; F.M. Calamunci, L. Ferrante and R. Scebba, "Closed for mafia: Evidence from the removal of mafia firms on commercial property values", (2022) 62(5) *Journal of Regional Science*, 1487–1511; G. Giorgi, "Der Kampf gegen die Mafia", *mafianeindanke*, 6 March 2019, <https://mafianeindanke.de/de/der-kampf-gegen-die-mafia/>.
- 15 See ECtHR, 21.1.2025, *Claudia Garofalo against Italy*, Appl. no. 47269/18.
- 16 The Act is available at: <https://www.legislation.gov.uk/ukpga/2002/29/contents>.
- 17 This applies for England and Wales, but procedure is different in Scotland and Northern Ireland.
- 18 Y.C. Chang and D. Klerman, "Settlement around the world: Settlement rates in the largest economies", (2022) 14(1) *Journal of Legal Analysis*, 80–175; R. Mulheron, "The Funding of the United Kingdom's Class Action at a Cross-Roads", (2023) *King's Law Journal*, 1–27.
- 19 K. Wegner, C. Ladwig, T. Zimmermann and M. El-Ghazi, "Vorschlag zur Einführung eines Gesetzes über das Aufspüren verdächtiger Vermögensgegenstände und über die selbständige Vermögenseinziehung (Vermögenseinziehungsgesetz)", *Kriminalpolitische Zeitschrift (KriPoZ)* 6/2022, 428–443, <https://kripoz.de/wp-content/uploads/2022/11/wegner-ladwig-zimmermann-el-ghazi-vorschlag-eines-vermoegenseinziehungsgesetzes.pdf>.
- 20 Therefore, the proposal by Wegner et. al. (op. cit. (n. 19)) serves as a comparative foil, not as the normative basis of the author's VEG.
- 21 § 75 *Gerichtsverfassungsgesetz* (Court Constitution Act); § 348 Abs. 1 ZPO.
- 22 The Deutsche Bundesbank is the central bank of the Federal Republic of Germany.
- 23 A multisig wallet is a crypto wallet that requires two or more signature to confirm and send a transaction, unlike traditional wallets, which require only one signature. For further understanding, see: bitpay (2025), "Using Multisig Wallets to Secure Your Crypto Assets", <https://www.bitpay.com/blog/multisig-wallet-security>.
- 24 M. Weber, G. Domeniconi, J. Chen, D.K. I. Weidele, C. Bellei,

**Dr. iur. Dr. rer. pol., Fabian M. Teichmann, LL.M. (London), EMBA (Oxford)**  
Rechtsanwalt und Notar / Attorney-at-Law  
Managing Partner Teichmann International (Schweiz) AG



- T. Robinson and C. E. Leiserson, "Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics", *arXiv:1908.02591*, <https://arxiv.org/pdf/1908.02591>.
- 25 § 15 II VEG-E, analogue §§ 2 ff. StrEG.
- 26 A Hardship clause allows for adjustments in agreements, see: cobrief (2025), "Hardship clause: Overview, definition and example", <https://www.cobrief.app/resources/legal-glossary/hardship-clause-overview-definition-and-example/>.
- 27 Gov.UK (2024), Asset recovery statistical bulletin: financial years ending 2019 to 2024, <https://www.gov.uk/government/statistics/asset-recovery-statistics-financial-years-ending-2019-to-2024/asset-recovery-statistical-bulletin-financial-years-ending-2019-to-2024>.
- 28 Y. Chistyakova, D. S. Wall & S. Bonino, "The back-door governance of crime: confiscating criminal assets in the UK, (2021) 27(4) *European Journal on Criminal Policy and Research*, 495–515; A. Owen, M. Nizzero & A. Larkin, "Seizing Crypto: When Asset Recovery Goes Digital", *RUSI*, 13 June 2024 <https://www.rusi.org/explore-our-research/publications/commentary/seizing-crypto-when-asset-recovery-goes-digital>.
- 29 Eigenössische Finanzkontrolle [Swiss Federal Audit Office], *Verwaltung der beschlagnahmten Güter – Querschnittsprüfung* [Report on Management of seized assets], SFAO-16606, 2018, [https://www.efk.admin.ch/wp-content/uploads/publikationen/berichte/sicherheit\\_und\\_umwelt/justiz\\_und\\_polizei/16606/16606be\\_endgultige\\_fassung\\_v04.pdf](https://www.efk.admin.ch/wp-content/uploads/publikationen/berichte/sicherheit_und_umwelt/justiz_und_polizei/16606/16606be_endgultige_fassung_v04.pdf).
- 30 Cf. Bundesverfassungsgericht [Federal Constitutional Court] BVerfG, 14 January 2004, 2 BvR 564/95; Official Case Reports E 110, 1, also available at: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/01/rs20040114\\_2bvr056495.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/01/rs20040114_2bvr056495.html); N. Nestler, "Zur Reichweite von § 73d StGB: Der erweiterte Verfall vor neuen Legitimationsdefiziten?", (2011) HRRS, 519 <https://www.hrr-strafrecht.de/hrr/archiv/11-12/index.php?sz=8>.
- 31 BVerfG, 7 June 2005, 2 BvR 1822/04, [https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2005/06/rk20050607\\_2bvr182204.pdf?\\_\\_blob=publicationFile&v=1&utm\\_source=.com](https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2005/06/rk20050607_2bvr182204.pdf?__blob=publicationFile&v=1&utm_source=.com).
- 32 Cf. BVerfG, 7 December 2022, 2 BvR 988/16, Official Case Reports E 164, 347, para. 159 ff., also available at: [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2022/12/rs20221207\\_2bvr098816.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2022/12/rs20221207_2bvr098816.html).
- 33 European Commission, Report from the Commission to the European Parliament and the Council based on Article 22 of the Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders, COM(2010) 428.
- 34 K. Fallon, O. Noble and K. Reynolds, "Institutional Owners in Single-Family Rental Properties – A Review of the Federal and Local Regulation and Policy Landscape", *Urban Institute*, August 2023, <https://www.urban.org/sites/default/files/2023-08/Institutional%20Owners%20in%20Single-Family%20Rental%20Properties.pdf>.

# Regulating Political Advertising in the EU

## Transparency Without Accountability

Randall Stephenson, Johanna Rinceanu, and Marc André Bovermann

In April 2024, the European Union's Regulation on the Transparency and Targeting of Political Advertising (PAR) entered into force. In further efforts to ensure a transparent, safe, predictable and trustworthy online environment within the EU — particularly in the wake of the Cambridge Analytica scandal — the Regulation aims to respond to the dangers and misuse of microtargeting, a sophisticated data-based method of online manipulation. Despite PAR's lofty aspirations, the nature and functions of online manipulation are fraught with more conceptual and regulatory difficulties than it appears to acknowledge or resolve. First, PAR's reliance on outmoded data protection principles and their largely unforeseeable effects on data disposition and aggregation complicate the problem of online user consent. Second, without adopting a broader "supervisory perspective" for identifying harmful microtargeting and interest misalignment, PAR risks endorsing only transparency without accountability. Third, a noticeable regulatory loophole risks prompting a surge in unregulated political advertising through platforms' existing posting functionality. Finally, persistent undertheorising of the underlying nature and effects of microtargeting precludes a comprehensive evaluation of its broader social harms and compatibility with democratic principles. Building on our two previous *Digital Latrogenesis* and *Differential Diagnosis eucrim* publications, this article aims to further highlight and provoke thought and discussion about the more latent and structural challenges of global digital media regulation.

### I. Introduction

Our contemporary digital media landscape continues to exhibit unforeseen regulatory tensions and harms. Perhaps most revealing is the phenomenon of *microtargeting*,<sup>1</sup> a sophisticated data-based method of online manipulation.<sup>2</sup> Though first arising in commercial settings, the upsurge in such techniques — especially psychographic profiling using machine learning and artificial intelligence (AI)<sup>3</sup> — now encompasses a growing *political* dimension evidenced by the rise of personalised advertising. The threats of this darker side of democracy's "algorithmic turn" are evidenced by the notorious Cambridge Analytica scandal,<sup>4</sup> which exposed the firm's misuse of Facebook data, and its suspected high-jacking of the Brexit referendum and the 2016 US Presidential election.<sup>5</sup> For those initially unpersuaded of microtargeting's dangers and misuse, its reach and powers have only intensified over the years. Besides being an obvious affront to personal autonomy and privacy, its seldom acknowledged aims of extracting hidden data and surprising correlations — and turning such sensitive information into votes — presents unprecedented structural risks to our democracies. Prompting concerns with election insecurity, digital repression, and disinformation,<sup>6</sup> this risky and scarcely understood technology also challenges uncritical use of regulatory approaches based on conventional data protection principles, and continued reliance upon overly-narrow definitions of "data-driven" harms.

The EU has been among the first responders. Its recent Regulation on the Transparency and Targeting of Political

Advertising (PAR) entered into force on 9 April 2024.<sup>7</sup> Besides prioritising privacy and personal data protection, PAR's numerous recitals allude to additional objectives of strengthening democracy and safeguarding electoral integrity. Despite Strasbourg Court jurisprudence limiting EU regulatory intervention in Member States' approaches to paid political advertising,<sup>8</sup> PAR nonetheless aims to harmonise "transparency" requirements as a central aspect of doing so.<sup>9</sup> This new harmonising measure complements a wide range of existing online regulations, including the Digital Services Act (DSA),<sup>10</sup> the Digital Markets Act (DMA),<sup>11</sup> and the General Data Protection Regulation (GDPR).<sup>12</sup> Overall, as explored in our earlier *Digital Latrogenesis* and *Differential Diagnosis eucrim* articles<sup>13</sup> — which aimed to highlight and provoke thought and discussion about the more latent and structural challenges of digital media regulation — PAR purports to add yet another piece to the broader regulatory puzzle of ensuring a safer digital environment in which EU online users' fundamental rights are protected. But does it?

Despite rising awareness of the internet's use as a powerful surveillance, profiling, and advertising tool,<sup>14</sup> scholarship germane to this matter suggests that the nature and functions of online manipulation pose more conceptual and regulatory challenges than PAR acknowledges or resolves. As shown below in Sections II to V, our analysis of this scholarship raises the following four criticisms of PAR's regulatory approach. First, PAR's reliance on outmoded data paradigms and their largely unforeseeable effects

on data disposition (and aggregation) complicate the problem of user consent. Second, unless a broader “supervisory perspective” or radical form of third-party-led data oversight is adopted, PAR risks (ironically) endorsing only transparency *without* accountability. Third, a noticeable regulatory loophole risks prompting a surge in unregulated political advertising through platforms’ existing posting functionality. Finally, persistent undertheorising of microtargeting’s underlying nature and effects precludes a comprehensive evaluation of its broader social harms and compatibility with democratic principles.

## II. Nature and Harms of Political Microtargeting

Before assessing PAR’s specific regulatory aims and approach, it is important to review the nature of political microtargeting, the vital preconditions for its emergence, and its growing harms to individuals and society.

### 1. Nature and emergence of microtargeting

#### a) Online manipulation

It is essential to first distinguish political microtargeting from other forms of influence. Privacy scholars have coined the term “online manipulation” to highlight the many concealed practices enabled by today’s rapidly evolving digital media environment. Whether considering Facebook’s microtargeting of vulnerable teenagers,<sup>15</sup> Uber’s algorithmic profit nudging of its labour force,<sup>16</sup> or Cambridge Analytica’s early use of psychographic profiling to manipulate electoral outcomes,<sup>17</sup> common to each is the exercise of *hidden* influence – the covert subversion of another person’s decision-making power. Compared to *persuasion*, which appeals to conscious deliberation, or *coercion*, which materially restricts one’s options, *manipulation* exploits another’s weaknesses and vulnerabilities to steer their decision-making process towards the manipulator’s ends. As a longstanding but underestimated example of online manipulation, microtargeting involves a deliberate *misalignment* of user interests.

#### b) Informational asymmetries and *laissez-faire* data disposition

While almost anyone can deceive (e.g. commit fraud), online manipulation requires a large power or knowledge imbalance rendering individuals susceptible to exploitation. It is therefore not surprising that microtargeting flourishes in today’s digital media ecology, which is typified by acute *informational asymmetries* and a particularly *laissez-faire*

regulatory approach to the flow and protection of disclosed information. Besides the data we shed “voluntarily” on social media, digital platforms’ dynamic, interactive, intrusive, and highly-personalisable choice architecture makes them an unprecedentedly powerful tool for hyper-targeted manipulation.

#### c) Outmoded data paradigms

This informational imbalance gives rise to a distinct regulatory anomaly, where data traffickers and digital platforms, whose interests may not align with those of their users, have both the intimate knowledge and relational proximity necessary to *manipulate* them commercially and politically. This anomaly is effectively explained by the principle of “privacy-as-concealment”.<sup>18</sup> Described as the “original sin” of the digital market,<sup>19</sup> this equates privacy with consumers’ ability to conceal information. Once information is “disclosed” online, users are treated as having *relinquished* their privacy and any reasonable expectation of data control. Except for persons having directly contracted with consumer-facing firms, disclosed information is generally *not* regulated and may be aggregated and sold freely.<sup>20</sup> This has become problematic as data traffickers’ secondary use of information lacks transparency, and thereby harms users in potentially uncontrollable ways. These data traffickers (or aggregators) have no interaction or privity of contract with persons they target, and arguably represent the “real engine” of online manipulation. Scholars caution that focussing regulatory efforts only on platforms’ Terms of Use merely facilitates outsourcing poor data practices to ungoverned third parties.<sup>21</sup>

### 2. From explicit to informed consent

Making matters worse, the largely unforeseeable effects of informational asymmetries and data disposition also complicate issues of consent, provoking calls for more stringent requirements analogous to the medical doctrine of *informed consent*.<sup>22</sup> According to this doctrine, consent must be “knowledgeable” in some meaningful sense in order to ensure awareness and to protect an individual’s ability to make autonomous decisions. Much like physicians disclosing detailed information vital to a patient’s decision about proposed treatment and interventions, digital platforms should provide online users with a summary in plain language of potential risks and benefits associated with data disposition (including political microtargeting).<sup>23</sup> This would enable users to give meaningful consent to any data disclosure. “Explicit consent”, hence, is not sufficient, particularly if users are unaware of a potentially harmful secondary (or even tertiary) use of their data. Arguably only in-

formed consent is capable of mitigating such informational imbalances (which enable digital platforms to *exploit* their data subjects), and protecting the self-determination of online users.

### 3. Microtargeting as a data-driven harm

Lastly, reflexively framing data misuse within individual privacy norms is increasingly seen as an “outdated paradigm” that overlooks rising structural threats to democracy. Since election interference and voter manipulation are harms affecting public interests, privacy is no longer just an individual issue, but a *networked* phenomenon requiring networked solutions.<sup>24</sup> Alongside calls to reconceptualise cybersecurity law and the “strict tangibility approach” to data-breach jurisprudence,<sup>25</sup> scholars have endorsed a *collective perspective* for regulating data-driven harms.<sup>26</sup> Aiming at “meaningful transparency”,<sup>27</sup> this requires far more than just disclosing ad-targeting criteria or funding details, or creating public ad-databases divorced from the harmful effects of data loops. Rather, a broader “supervisory perspective” is needed to *correlate* outgoing user information with incoming personalised content in order to identify harmful commercial and political microtargeting and interest misalignment.<sup>28</sup> This heightened informational scrutiny, however, leads to a larger regulatory dilemma. As a prominent free speech scholar observed already in 2016, “the more speech-protective the government’s policy, the more hands-on the government’s approach will need to be”.<sup>29</sup> That is to say, a regulatory dilemma arises owing to such extreme forms of informational transparency. The very “supervisory perspective” needed for identifying and exposing microtargeting and interest misalignment unfortunately also confers unprecedented possibilities for privatised governmental censorship and regulatory capture. As opposed to earlier predigital eras, regulating online speech invariably places the government in our proverbial editorial office. Ironically, without this extreme level of informational surveillance, regulatory proposals such as PAR risk only endorsing transparency *without* accountability.

## III. PAR’s Essential Aims and Features

### 1. Regulatory aims

PAR aims to contribute to the proper functioning of the EU’s internal market for political advertising, and to protect fundamental rights and freedoms – particularly the right to privacy and the protection of personal data (Art. 1(4) PAR). Responding to digital technologies and the use of social media in electoral campaigning that offer political actors massive reach at low cost,<sup>30</sup> PAR introduces harmonised

transparency rules regarding online political campaigning for each of the EU’s 27 Member States.

### 2. Regulatory features

Despite its apparent complexity, PAR comprises four main regulatory features: (1) labelling and transparency requirements; (2) establishing a public database for political ads; (3) restricting political microtargeting and foreign electoral interference; and (4) sanctioning non-compliance.

First, political ads must be clearly labelled and include an easily retrievable notice disclosing details such as its sponsor, any controlling entity, the electoral process to which the ad refers, the amounts paid, and any microtargeting or ad-delivery methods used (Arts. 11, 12 PAR). Notices must be accessible contemporaneously with the original ad (e.g. via QR-Code) and (like DSA) provide a “notice-and-action” mechanism for reporting non-compliant ads (Art. 15 PAR).

Second, both the ad and notice must be submitted to a European repository established by the Commission (Art. 13 PAR) – a public database available in machine-readable format. If the publisher is a very large online platform (VLOP) within the meaning of Art. 33 DSA, it can use its general ad repository. However, as with all PAR record-keeping, VLOPs must facilitate access for seven years after the ad was last posted (Arts. 12(4), 13 PAR).

Third, PAR permits targeted online political advertising, subject to three conditions (Art. 18 PAR): (1) the controller (i.e. data processing entity) must collect the personal data *directly* from the subject; (2) the latter must *explicitly consent* to the processing of their personal data for political advertising; and (3) the processing cannot involve “profiling” (i.e. “any form of automated processing of personal data”) using special data categories (e.g. race or ethnicity, political opinions, etc.) as referred to in Art. 9(1) GDPR. Importantly, PAR prohibits political microtargeting to minors (Art. 18(2) PAR). Foreign electoral interference is restricted by a so-called “silence period”, which prohibits provision of political advertising services to non-EU or otherwise unqualified foreign sponsors (or service providers) within three months of an election or referendum organised at EU, national, or regional levels (Art. 5(2) PAR).

Fourth, like the DSA, PAR imposes indexed financial penalties for non-compliance. Fines must not exceed 6% of the annual income or budget of the sponsor or the provider of political advertising services (as applicable), or 6% of the sponsor’s or provider’s annual worldwide turnover in the preceding financial year (Art. 25 PAR).



#### IV. Political Advertising's "Regulatory Loophole"

This is about where regulatory certainties end as PAR's scope of application seems unclear in one important respect. A close look at the definition of "political advertising service" in Art. 3(5) PAR reveals a drafting irregularity that appears to obscure PAR's regulatory reach. It reads:

'political advertising service' means a service consisting of political advertising with the exception of an online 'intermediary service', as defined in Article 3, point (g), of Regulation (EU) 2022/2065, that is provided without consideration, for the preparation, placement, promotion, publication, delivery or dissemination for the specific message.

The source of ambiguity originates from the attempt to exempt "intermediary services" from the definition of "political advertising service". Notably, Art. 3(g) DSA divides "intermediary services" into three distinct categories: (1) "mere conduit" service; (2) "caching" service; and (3) "hosting" service (e.g. social media platforms).

Difficulty arises when attempting to discern what the words "provided without consideration" modify. If interpreted to restrict the definition of "political advertising service", a tension arises between the categorical exclusion of conduit, caching, and hosting intermediaries, and the further obligation to saddle "political advertising publishers" (defined in (Art. 3(13)) with the full suite of transparency obligations under PAR. While mere conduit and caching services (i.e. non-curatorial) – along with purely private and purely commercial messages – are clearly and understandably exempt from PAR's application, exempting "hosting services" captured by the definition of "political advertising publisher" makes considerably less sense.

By contrast, if "provided without consideration" modifies the exempted online "intermediary services" (under DSA), a crucial policy factor comes back into focus. Specifically, this interpretation is consistent with the reassurance in Recital 47 that PAR should *not* apply to *unpaid* content uploaded by users of an online intermediary (e.g. hosting) service, such as a social media platform. In short: no paid "political advertising service", no transparency obligations. So, why rely on political advertising services when one could simply use a platform's basic posting functionality? As the following two examples show, this regulatory loophole has already generated serious socio-political consequences.

First, as political campaigns increasingly take place in the digital sphere, modern electioneering is not merely conducted through ad-distribution services, but involves direct engagement with potential voters on politicians' home turf – namely, on their own private social media feeds. The po-

litical right has mastered this type of voter engagement.<sup>31</sup> In Germany, a good example is *Maximilian Krah* of the *Alternative für Deutschland* (AfD) party, who has gathered a huge audience on TikTok. As Krah's growing popularity and the last German federal election have shown,<sup>32</sup> PAR risks inadvertently prompting a surge in unregulated political advertising through the existing posting function on platforms.

Second, the use of TikTok by Romanian presidential candidate *Călin Georgescu* has sparked a debate about digital campaigning in the context of the last Romanian presidential election. The election was annulled by the Romanian Constitutional Court.<sup>33</sup> It commented on Georgescu's use of his personal TikTok account to influence voters and held that the presidential electoral process had been subverted. The Court emphasised that Georgescu had unfairly benefited from aggressively promoting his political messages through digital platforms' algorithms, which had effectively circumvented the electoral legislation and led to misinformation and voter manipulation.<sup>34</sup>

In the end, despite PAR's explicit commitment to "fully respect fundamental rights" in its objectives and application, this regulatory loophole not only inadvertently emboldens right-wing populist parties and candidates, but also appears to pose a considerable threat to the openness and accountability of EU electoral mechanisms.

#### V. Undertheorising Democratic Free Speech Rationales

Besides uncertainties about its application, PAR also raises vital fundamental rights concerns. As commentators acknowledged early on in the regulatory debate about online manipulation, "[b]ecause of free speech norms, policymakers must tread carefully when regulating political speech, and when regulating political advertising".<sup>35</sup> While the scholarly literature on the nature and suitability of political microtargeting – and "online manipulation" more generally – invokes conventional free speech conceptions of autonomy, chilling effects,<sup>36</sup> and participatory and deliberative democracy, this scholarly discussion remains undertheorised and therefore regulatorily deficient in one key respect. Specifically, as with other areas of freedom of expression regulation – public libel law<sup>37</sup> being especially illustrative – existing scholarship consistently overlooks perhaps the most relevant free expression justification for regulating the threats of political microtargeting: the "checking function" rationale and its link to democratic accountability.<sup>38</sup> This undertheorising manifests in two distinct but related ways pertinent to regulators on both sides of the Atlantic.



## 1. Conflating democratic free-speech values

The first form of undertheorising involves scholarly attempts to expand “data-driven” harms to include those affecting democracy more broadly, where the scalable effects of online manipulation are routinely (and imprudently) masked by subsuming the checking function within classic *Meiklejohnian* notions of deliberative democracy.<sup>39</sup> The upshot is a disproportionate focus on free speech’s “information conduit” role in *imparting* and *receiving* information – as guaranteed under Art. 10 of the European Convention on Human Rights (ECHR) and Art. 11 of the Charter of Fundamental Rights of the European Union (Charter) – rather than minding the impact of PAR’s “harmonising” strategy on the institutional press’ vital *watchdog* role of holding power to account. Whether purporting to assess political microtargeting’s advantages and disadvantages,<sup>40</sup> or the inevitable “trade-offs” between different and often conflicting democratic values and ideas,<sup>41</sup> a vital shortcoming of regulatory analyses is the systematic disregard of the checking function rationale – a crucial component in achieving a precise regulatory balance between competing rights, interests, and values. In effect, by overlooking the checking function and its connection to the press’ vital but waning “fourth estate” role,<sup>42</sup> when one explicitly acknowledges political microtargeting’s hidden and manipulative nature, regulatory evaluations necessarily understate its harmful socio-political effects on democracy.

This undertheorising can have serious and disruptive regulatory and doctrinal outcomes. As recent comparative law scholarship has revealed, “our ability to diagnose and understand contemporary problems falters when we encounter breakdowns in the theory-doctrine interface”.<sup>43</sup> As reported in the comparable context of online defamation, our strongest guarantee of sound regulation and doctrine “depends on ensuring a complete inventory of fully articulated free expression justifications carefully applied to relevant issues and disputes. The effects of the Internet, however measured, cannot sidestep this basic requirement”.<sup>44</sup> As threatened in the context of PAR’s regulatory approach to political microtargeting, at stake is no less than the likelihood of inadvertently promoting arbitrary regulatory measures at odds with our most fundamental political values.

## 2. Political microtargeting as “speech”

A further form of undertheorising is raised by reflexively interpreting political microtargeting as a protected form of political communication or “speech”, a disquieting scholarly approach seen both in Europe and North America.<sup>45</sup> Importantly, whether in either context, if microtargeting is uncriti-

cally presumed to be political “speech”, our regulatory focus will remain elsewhere than on tracking its fundamental inconsistency with underlying freedom of expression justifications, particularly the checking function rationale.

As a recent commentary on the nature and threats of political microtargeting has shown,<sup>46</sup> a key component of its proper regulation will be engaging in a careful assessment of its doctrinal and theoretical status as a form of protected speech. Despite temptations to *equate* political microtargeting with political communication, or to interpret it in a *Meiklejohnian* manner consistent with notions of deliberative democracy and the basic structure of Art. 10 ECHR and Art. 11 of the Charter (i.e. as the dyadic *imparting* and *receiving* of information),<sup>47</sup> a recent vein of scholarship on algorithms’ status as “protected speech” has sensibly advised *against* such presumptive views.

In the context of US First Amendment doctrine, Columbia Law Professor *Tim Wu* has convincingly argued that the law contains a “de facto *functionality* doctrine” that “must be central to any consideration of [regulating] machine speech”.<sup>48</sup> In other words, in the absence of any suspicious governmental censorship motives, this “functionality doctrine” will be the main dividing line between constitutionally protected “speech” and other forms of communication. This doctrine, according to *Wu*, operates in two distinct ways.

The first category of information excluded from First Amendment protection is where it is simply “too distant or mechanical to be speech”.<sup>49</sup> *Wu* explains that this covers those who handle or transform information in a *non-curatorial* manner “usually lacking specific choices as to content, [who] lack specific knowledge as to what they are handling, or do not identify as the publisher of the information”.<sup>50</sup> Telephone services, for example, have historically fallen outside the ambit of free speech rights as they were treated as essential utilities, not as “speakers”. The second category of excluded speech are “communicative tools”, where the information conveyed is *functional* – viz., it performs some task *other than* the communication of ideas. *Wu* references both ordinary maps and navigational charts as paradigmatic examples of such “communicative tools”. In the end, the largely unstated reasons courts give for denying constitutional protection to non-curatorial carriers or communicative tools, is their reluctance to extend free speech regulation into areas where other motivations are paramount and/or to quell the opportunism of lawyers trying to use the Constitution to achieve goals unrelated to speech.<sup>51</sup>

Furthermore, without incorporating this functionality doctrine as a missing regulatory piece of the puzzle, uncritical

and reflexive application of the now decades-old “code is speech”- model will continue to yield results both absurd and disruptive that cannot be taken seriously. Interestingly, in a bid to “roll back” the regulatory overestimation of “[...] the significance of computer code’s superficial resemblance to words on a page”,<sup>52</sup> and to prevent further overprotection of computer code secured during the first wave of internet cases, free speech scholar *Kyle Langvardt* has recommended adopting a “threshold test” patterned on Wu’s “functionality doctrine”. This would work by “quarantining” new code cases (e.g. those involving algorithms and machine learning) from “mainline First Amendment doctrine so that they are not decided under the same set of [overbroad] tests”.<sup>53</sup> As this discussion shows, deciding that political microtargeting constitutes “political speech” involves a considerably more complex and careful analysis, whether in European or American jurisdictions.

At last, just as framing data misuse within conventional privacy norms has been criticised as an “outmoded paradigm” that neglects growing harms to democracies, this narrowing of democratic free speech rationales (and over-constitutionalising of computer code) risks greatly limiting our understanding of the full extent and severity of political microtargeting. This theoretical oversight obscures the reasons *why* we should be concerned with its regulation and/or outright prohibition in the first place.

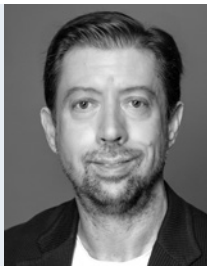
## VI. Conclusion

Which brings us full circle. Viewed in light of the scholarly foundations of microtargeting, PAR’s regulatory approach (and even mere existence) raises many questions, in the end overpromising and underdelivering on its avowed policy aims. First, despite the apparent lack of regulatory fragmentation that would justify the EU’s push to “harmonise” transparency obligations,<sup>54</sup> PAR’s reliance on conventional data protection paradigms and limited regulatory reach effectively endorses only transparency without accountability. With the exception of bald compliance (re)assurances in regulated entities’ annual reports, harmful political microtargeting and interest misalignment will in all likelihood remain undetected unless a collective perspective that correlates outgoing user data with incoming personalised content is adopted. Second, PAR continues to overlook the insufficiency of existing user “consent” requirements. Whether confronted with personalised content or not, it remains unclear how users can meaningfully (let alone “explicitly”) consent to unforeseeable secondary (and even tertiary) data aggregation, disposition, and manipulation. Third, as evidenced by Maximilian Krah and Călin Georgescu’s use of their pri-

vate social media feeds, a noticeable regulatory loophole risks prompting a surge in unregulated political advertising through platforms’ existing posting functionality. Finally, this article has explained that persistent undertheorising of microtargeting’s harmful effects precludes a full evaluation of its compatibility with democratic principles. While digital media regulation inevitably involves trade-offs between different and often competing democratic values, it is difficult to determine which regulatory approach best serves democracy, or even which understanding of democracy should prevail, without fully canvassing the nature and implications of *each* rationale. Under such circumstances, PAR’s overall approach, expected benefits, and effects are in the end far from clear.

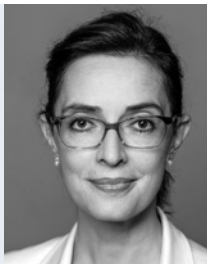
**Dr. Randall Stephenson, LL.M. (Columbia),  
M.St., D.Phil. (Oxon)**

Senior Researcher, Public Law Department,  
Max Planck Institute for the Study of Crime,  
Security and Law, Freiburg i.Br., Germany



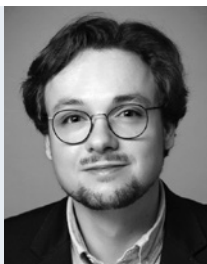
**Dr. Johanna Rinceanu, LL.M. (Washington, D.C.)**

Senior Researcher, Criminal Law  
Department, Max Planck Institute for the  
Study of Crime, Security and Law, Freiburg  
i.Br., Germany



**Marc André Bovermann**

Doctoral Researcher, Public Law  
Department, Max Planck Institute for the  
Study of Crime, Security and Law, Freiburg  
i.Br., Germany



1 See generally N. Witzleb, M. Paterson and J. Richardson, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting*, 2021.

2 See D. Susser, B. Roessler and H. Nissenbaum, “Online Manipulation: Hidden Influences in a Digital World”, (2019) 4 *Georgetown Law Technology Review*, 1.

3 D. Susser and others, *op. cit.* (n. 2), 9–12. See also “Psychographic Profiling: The Secret to Enhanced Marketing”, *Sagacity*, <<https://www.sagacitysolutions.co.uk/about/news-and-blog/psychographic-profiling-the-secret-to-enhanced-marketing/>>. All

hyperlinks in this article were last accessed on 4 July 2025.

- 4 See e.g., A. Gurumurthy and D. Bharthur, "Democracy and the Algorithmic Turn", (2018) 27 *SUR – International Journal on Human Rights*, 39.
- 5 See e.g., A. Chan, "Cambridge Analytica and our Lives Inside the Surveillance Machine", *The New Yorker*, 21 March 2018, <<https://www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine>>.
- 6 See generally S. Shackelford, A. Raymond, A. Stemler and C. Loyle, "Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity", (2020) 77 *Washington & Lee Law Review*, 1747.
- 7 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency of political advertising, *OJ L*, 2024/900, 20.3.2024.
- 8 M. Zeno van Drunen, N. Helberger and R. Ó Fathaigh, "The beginning of EU political advertising law: unifying democratic visions through the internal market", (2022) 30 *International Journal of Law and Information Technology*, 181, 182, citing *Animal Defenders International v United Kingdom* [2013] ECtHR 48876/08 [123]; *VgT Verein gegen Tierfabriken v Switzerland* [2001] ECtHR 24699/94 [70]; *TV Vest* [2008] ECtHR 21132/05 [67].
- 9 M. Zeno van Drunen and others, *op. cit.* (n. 8), 195–96. The authors rightly noted that there appears to be insufficient regulatory fragmentation to justify the EU's push to "harmonise" transparency obligations. Hypothesising that "transparency [is] an area Member States were most likely to accept European Commission intervention," they emphasised that "[t]his still leaves the question, unaddressed by the impact statement, why the regulation of transparency is available for harmonization but other areas not [...]" (p. 196). Given the large scope of discretion granted to Member States, PAR would appear to be regulating their domestic political affairs under the mere guise of transparency.
- 10 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] *OJ L*1277/1.
- 11 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
- 12 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 (General Data Protection Regulation).
- 13 R. Stephenson and J. Rinceanu, "Digital latrogenesis: Towards an Integrative Model of Internet Regulation", (2023) 1 *eu crim*, 73; R. Stephenson and J. Rinceanu, "Differential Diagnosis in Online Regulation: Reframing Canada's 'Systems-Based' Approach", (2024) 3 *eu crim*, 245.
- 14 See S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019.
- 15 S. Levin, "Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'", *The Guardian*, 1 May 2017, <<https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>>.
- 16 Z. Muller, "Algorithmic Harms to Workers in the Platform Economy: The Case of Uber", (2020) 53 *Columbia Journal of Law and Social Problems*, 167.
- 17 S. Halpern, "Cambridge Analytica and the Perils of Psychographics", *The New Yorker*, 30 March 2018, <<https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics>>.
- 18 K. Martin, "Manipulation, Privacy, and Choice", (2022) 23 *North Carolina Journal of Law & Technology*, 452, 493.
- 19 K. Martin, *op. cit.* (n. 18), 494.
- 20 Emanuela Podda, "Shedding Light on the Legal Approach to Aggregate Data Under the GDPR & the FFDR" (Conference of European Statisticians – Expert Meeting on Statistical Data Confidentiality, Poland, December 2021). Citing Recital 162 of the GDPR, Podda states that "aggregate data is the result of personal data processing for statistical purpose (output data) and it is considered non-personal data". Interestingly, this position appears to be in tension with the principle of "integrity and confidentiality" under Art. 5(1)(f) GDPR.
- 21 K. Martin, *op. cit.* (n. 17), 520.
- 22 K. Rhum, "Information Fiduciaries and Political Microtargeting: A Legal Framework for Regulating Political Advertising on Digital Platforms", (2021) 115 *Northwestern University Law Review*, 1829, 1868.
- 23 K. Rhum, *op. cit.* (n. 22), 1868.
- 24 See J. Dawson, "Microtargeting as Information Warfare", (2021) 6 *Cyber Defense Review*, 63, 72.
- 25 See I. Kilovaty, "Legally Cognizable Manipulation", (2019) 34 *Berkeley Technology Law Journal*, 449, 459–60.
- 26 See A. Gordon-Tapeiro, A. Wood and K. Ligett, "The Case for Establishing a Collective Perspective to Address the Harms of Platform Personalization", (2023) 25 *Vanderbilt Journal of Entertainment and Technology Law*, 635.
- 27 A. Gordon-Tapeiro and others, *op. cit.* (n. 26), 679.
- 28 A. Gordon-Tapeiro and others, *op. cit.* (n. 26), 682.
- 29 See K. Langvardt, "Regulating Online Content Moderation", (2018) 106 *Georgetown Law Journal*, 1353, 1363.
- 30 K. Wirthwein, M. Cabañas, F. Di Nunno and L. Rea, "EU Regulation on Transparency and Targeting of Political Advertising – Could the New Legislation be Effective at Stopping Populism?", (FEPS Policy Study, April 2024), <<https://feps-europe.eu/wp-content/uploads/2024/05/PS-EU-regulation-on-transparency-DIGITAL.pdf>>.
- 31 See "So ungleich war der Bundestagswahlkampf im Netz", *Tagesschau*, 6 March 2025, <<https://www.tagesschau.de/investigativ/bundestagswahl-wahlwerbung-instagram-facebook-parteien-budget-100.html>>.
- 32 See e.g., Hans Pfeifer, "AfD: How Germany's far right won over young voters", *Deutsche Welle*, 10 June 2024, <<https://www.dw.com/en/afd-how-germanys-far-right-won-over-young-voters/a-69324954>>.
- 33 See Constitutional Court of Romania, decision no. 32/2024, published in M. Of. no. 1231 from 6 December 2024; ECtHR, 6 March 2025, *Georgescu v Romania*, Appl. no. 37327/24.
- 34 See Constitutional Court of Romania, *op. cit.* (n. 33), para. 14.
- 35 See generally F.J. Zuiderveen Borgesius, J. Möller, S. Kruike-meier, R. Ó Fathaigh, K. Irion, T. Dobber, B. Bodo and C. de Vreese, "Online Political Microtargeting: Promises and Threats for Democracy", (2018) 14 *Utrecht Law Review*, 82, where the authors' early attempt to assess the impact of political microtargeting is fundamentally led astray by overlooking the independent checking function rationale.
- 36 See e.g., *Baggett v Bullitt*, 377 US 360 (1964), where the US Supreme Court struck down a Washington state law mandating loyalty oaths for state employees, asserting that the "the threat of sanctions may deter [...] almost as potently as the actual application of sanctions".
- 37 See e.g., R. Stephenson, *A Crisis of Democratic Accountability: Public Libel Law and the Checking Function of the Press*, 2018.
- 38 See V. Blasi, "The Checking Value in First Amendment Theory", (1977) 2 *American Bar Foundation Research Journal*, 521.
- 39 See A. Meiklejohn, "Free Speech and its Relation to Self-Gov-

ernment", in A. Meiklejohn, *Political Freedom: The Constitutional Powers of the People*, p. 1948.

40 F.J. Zuiderveen and others, *op. cit.* (n. 35).

41 D. Kreiss and B. Barrett, "Democratic Tradeoffs: Platforms and Political Advertising", (2020) 16 *Ohio State Technology Law Journal*, 495.

42 For well-documented accounts of the recent crisis of journalism, see e.g., A.S. Jones, *Losing the News: The Future of the News that Feeds Democracy*, 2009; R.W. McChesney and J. Nichols, *The Death and Life of American Journalism: The Media Revolution That Will Begin the World Again*, 2010; David AL Levy and Rasmus Kleis Nielsen (eds.), *The Changing Business of Journalism and Its Implications for Democracy*, 2010; L.C. Bollinger, *Uninhibited, Robust, and Wide-Open: A Free Press for a New Century*, 2010, ch 3; R.W. McChesney and V. Pickard (eds.), *Will the Last Reporter Please Turn out the Lights: The Collapse of Journalism and What can be Done to Fix It*, 2011.

43 See R. Stephenson, "Restoring Accountability in Freedom of Expression Theory: Public Libel Law and Radical Whig Ideology", (2018) 56 *Osgoode Hall Law Journal*, 17, 57.

44 Stephenson, *op. cit.* (n. 43), 58.

45 T. Dobber, R. Ó Fathaigh and F.J. Zuiderveen Borgesius, "The Regulation of Online Political Micro-Targeting in Europe", (2019) 8(4) *Internet Policy Review*, 1, 7.

46 Dobber and others, *op. cit.* (n. 45).

47 Dobber and others, *op. cit.* (n. 45), 7.

48 T. Wu, "Machine Speech", (2013) 161 *University of Pennsylvania Law Review*, 1495, 1497. For an opposing view, see S.M. Benjamin, "Algorithms and Speech", (2013) 161 *University of Pennsylvania Law Review*, 1445, where the author maintains that algorithmic-based outputs that entail substantive editorial decisions are "speech" for First Amendment purposes.

49 Wu, *op. cit.* (n. 48), 1521.

50 Wu, *op. cit.* (n. 48), 1521.

51 Wu, *op. cit.* (n. 48), 1524.

52 K. Langvardt, "Four Modes of Speech Protection for Algorithms", in W. Barfield (ed.), *Cambridge Handbook of the Law of Algorithms*, 2020, 543, 557.

53 Langvardt, *op. cit.* (n. 52), 552.

54 M. Zeno van Drunen and others, *op. cit.* (n. 8), 195–96.

# Übersetzen und Dolmetschen im Rechtswesen

Tinka Reichmann

This article discusses different perspectives on translation and interpreting for courts and other organs of judicature in Germany. It draws on insights from translation studies and the law to offer a comprehensive examination of this subject. Despite productive research in legal translation studies and comparative law in recent decades, there is still a gap to bridge between the two fields: learning more from each other could improve daily translation and interpreting services and raise awareness of quality requirements and issues in interpreting and translation. German legislation has few dedicated provisions regarding the function and the scope of responsibility of translators and interpreters, and instead relies largely on extensive commentaries by legal scholars and on case law. Conversely, translation studies has been putting effort into developing tailored approaches where it intersects with legal disciplines – one example being juritraductology, which focuses on both the translation of legal texts and the "right of translation", i.e. legal aspects of translation and interpreting. Furthermore, the emerging discipline of juritraductology (Juritraductologie, Rechtstraductologie) expands the focus beyond mere legal text translation to encompass the "right to translation", including rights to interpretation and translation as mandated by EU Directives 2010/64/EU and 2012/13/EU in criminal proceedings.

## I. Einleitung

Übersetzen und Dolmetschen im Rechtsbereich ist ein weites Feld, das u. a. das Urkundenübersetzen und das Dolmetschen bei Gericht, Polizei, Notariaten, Staatsanwaltschaften, Justizvollzugsanstalten, unterschiedlichen Behörden und nicht zuletzt in der forensischen Psychiatrie umfasst. In der Berufspraxis stehen Übersetzer und Dolmetscher vor verschiedenen Herausforderungen, weil das juristische Fachpersonal in der Praxis nicht immer mit der Rolle und Tätigkeit von Übersetzern und Dolmetschern vertraut ist. Daher sollen in diesem Beitrag die wichtigsten Perspektiven auf beiden Seiten dargestellt und Verbesse-

rungsmöglichkeiten für die Zusammenarbeit aufgezeigt werden. Aufgrund der aktuellen Entfaltungen des Gerichtsdolmetschergesetzes (GDolmG)<sup>1</sup> wird in diesem Beitrag der Fokus vorrangig auf das Dolmetschen gelegt.

Die mit Hilfe von Übersetzern und Dolmetschern auf Sprachmittlung angewiesenen Institutionen sind mit der Tatsache konfrontiert, dass anerkannte Hochschulen in Deutschland nur Übersetzer und Dolmetscher in bestimmten Sprachen ausbilden und somit nicht die gesamte Palette an Sprachen und fachlichen Schwerpunkten (Jura, Technik, Medizin u.v.m) abdecken können. Ähnlich verhält es sich mit staatlichen Prüfungsämtern. Daher ziehen die Institutionen re-



gelmäßig Ad-hoc-Dolmetscher hinzu, die nicht allgemein beeidigt sind und somit nicht die im GDolmG formulierten Anforderungen erfüllen, u.a. die fachliche Qualifikation im Dolmetschen oder die „Grundkenntnisse der deutschen Rechtssprache“.<sup>2</sup> Gleichzeitig haben qualifizierte Dolmetscher Mühe, vor ihren Einsätzen Informationen über die jeweiligen Verfahren oder Akteneinsicht zu erhalten und wenden sich nach einiger Zeit oft vom Justizsektor ab, nicht zuletzt aufgrund der mangelnden Anerkennung und Wertschätzung.

Die Zusammenarbeit könnte insgesamt aber trotz all dieser Widrigkeiten verbessert werden, wenn Juristen mehr über das Dolmetschen und Übersetzen wüssten und Übersetzer und Dolmetscher mehr über die rechtliche Stellung und Funktion von Übersetzern, Dolmetschern und Sachverständigen. Dieser Beitrag stellt Überlegungen an, dieses gegenseitige Verständnis zu wecken oder zu vertiefen.

## II. Übersetzen und Dolmetschen aus translatologischer und translationspraktischer Sicht

Zunächst sind einige terminologische Klärungen zum Fachgebiet der Translatologie erforderlich, die sich wissenschaftlich mit den Phänomenen des Übersetzens und des Dolmetschens beschäftigt (auch „Translationswissenschaft“ genannt). Diese besteht aus verschiedenen Unterdisziplinen, so z. B. Übersetzungswissenschaft, Dolmetschwissenschaft, Soziotranslatologie, Historiographie der Translation, Übersetzungstechnologien, mehrsprachige Terminologie und Terminographie, digitale Translatologie und die in dem vorliegenden Kontext einschlägige Rechtstranslatologie.<sup>3</sup> Letztere steht an der Schnittstelle zwischen Rechtsvergleichung, Rechtslinguistik und Translatologie.<sup>4</sup> Die Translation des Rechts (*Traduction du Droit*) bezeichnet die Übertragung von rechtlichen Inhalten in andere Sprachen, während das Recht der Translation (*Droit de la Traduction*) die Gesamtheit der Rechtsnormen und Rechtsprechung umfasst, die sich auf die Tätigkeit des Übersetzens und Dolmetschens beziehen, insbesondere auch das Recht auf Translation.<sup>5</sup> „Translation“ ist der Oberbegriff für das Übersetzen und das Dolmetschen. Das Verb „übertragen“ wird für beide Tätigkeiten verwendet, wobei es auch im Dolmetschereid nach § 189 Gerichtsverfassungsgesetz (GVG) Erwähnung findet. Der Leipziger Translatologe *Otto Kade* definiert das Übersetzen als die „Translation eines fixierten und demzufolge permanent dargebotenen bzw. beliebig oft wiederholbaren Textes der Ausgangssprache in einen jederzeit kontrollierbaren und wiederholt korrigierbaren Text der Zielsprache“.<sup>6</sup> Das Dolmetschen definiert er als die „Translation eines einmalig (in der Regel mündlich) dargebotenen Textes der Ausgangs-

sprache in einen nur bedingt kontrollierbaren und infolge Zeitmangels kaum korrigierbaren Text der Zielsprache“.<sup>7</sup> Der österreichische Translatologe *Erich Prunč* präzisiert noch, dass beim Übersetzen die „Möglichkeit des multiplen Zuganges zum AT [Ausgangstext] und ZT [Zieltext]“<sup>8</sup> bestehe und beim Dolmetschen eben nicht, weil hier der Zugang zum Text linear ist. Ein Übersetzer kann also einen Text querlesen und von einer Textstelle zu einer anderen springen, während Dolmetscher den Ausgangstext nur in der einmaligen, linearen Abfolge der tatsächlichen Darbietung rezipieren können.

Es gibt aber auch hybride Translationsmodi an der Schnittstelle zwischen Mündlichkeit und Schriftlichkeit, wie z. B. das „Vom-Blatt-Dolmetschen“ (mündliche Übertragung in eine andere Sprache auf der Grundlage eines schriftlichen Texts) oder die Translation von Audio-Aufzeichnungen im Rahmen von polizeilichen Ermittlungen, insbesondere bei der Telekommunikationsüberwachung. Hierbei wird ausgehend von Aufzeichnungen mündlicher Äußerungen in einer Fremdsprache eine schriftliche Übersetzung in die Landessprache angefertigt.

Die Translatologie hat ihren Ursprung als wissenschaftliche Disziplin in den 1960er Jahren und stützte sich anfangs vorrangig auf linguistische Kategorien. Nach und nach wurde das Tätigkeitsfeld durch Austausch mit anderen (verwandten) Bereichen erweitert (Terminologie und Terminographie, Psychologie, Textsortenlinguistik, kontrastive Linguistik, Fachkommunikationsforschung, Fachstilistik, Kulturwissenschaft u. a.). Im Fokus standen Übersetzungsmethoden, die Suche nach Äquivalenzen auf verschiedenen Ebenen, Kriterien der Übersetzungsqualität und empirische Untersuchungen in den verschiedensten Anwendungsgebieten.

Rechtstexte gelten als stark kulturspezifisch geprägt, weil es bei der Translation nicht nur um die zwei beteiligten Sprachen geht, sondern auch um die jeweiligen Rechtsordnungen. So sind beispielsweise Rechtstermini und die darin enthaltenen Konzepte jeweils in einer nationalen Rechtsordnung verortet, weshalb es trotz einer gleichen Amtssprache erhebliche inhaltlichen Abweichungen geben kann (z. B. Frankreich/Tunesien, Portugal/Brasilien oder Österreich/Deutschland). Die kulturspezifische Dimension äußert sich auf verschiedenen Ebenen: lexikalisch (als unübersetzbar geltende rechtskulturgebundene Termini), textuell (Textsorten und Vertextungskonventionen) und diskursiv (unterschiedliche juristische Diskurs-traditionen). Die Interdisziplinarität, welche die Translatologie kennzeichnet, führt auf wissenschaftlicher Ebene zu Schnittstellen mit Disziplinen wie der Rechtslinguistik,<sup>9</sup>



der Rechtsvergleichung<sup>10</sup> und verschiedenen Bereichen der Linguistik. Die Perspektiven der Rechtstranlatologie reichen von der mikrostrukturellen Ebene (z. B. Rechtsterminologie) über juristische Textsorten hin zur Verständlichkeit von Rechtsnormen, der Verwendung institutioneller Sprache (u. a. in supranationalen Institutionen) und Fragen der Übersetzbarkeit, Übersetzungsmethoden und Äquivalenz. Das Dolmetschen fristete lange Zeit eher ein Randdasein, inzwischen haben sich Übersetzungswissenschaft und Dolmetschwissenschaft als zwei verwandte, aber doch getrennte Disziplinen in Forschung und Lehre etabliert.

### III. Übersetzen und Dolmetschen aus rechtlicher Sicht

#### 1. Bestimmungen im deutschen Recht

Es ist für Translatoren überraschend, dass es relativ wenige gesetzliche Regelungen zur Stellung und Tätigkeit von Dolmetschern und Übersetzern im Recht gibt. Zu nennen sind §§ 185 ff. des Gerichtsverfassungsgesetzes (GVG), das Gerichtsdolmetschergesetz und vereinzelte Vorschriften in Verfahrensordnungen, wie z. B. § 142 Zivilprozessordnung (ZPO) oder § 259 Strafprozessordnung (StPO). Die gesetzlichen Regelungen werden durch Gesetzeskommentare, Rechtsprechung, Rechtsgutachten und rechtswissenschaftliche Literatur ergänzt, um die Stellung und Tätigkeit von Dolmetschern und Übersetzern zu definieren.<sup>11</sup> So wird z. B. bis heute noch für die Beschreibung der Tätigkeit von Gerichtsdolmetschern ein grundlegendes Urteil des Bundesgerichtshofs (BGH) von 1950 herangezogen:<sup>12</sup> „**Dolmetscher** ist ein Sprachkundiger, dessen Aufgabe es ist, den Prozeßverkehr zwischen dem Gericht und anderen am Prozeß beteiligten Personen zu ermöglichen.“

Diese Definition greift eindeutig zu kurz. Das Oberlandesgericht (OLG) Schleswig hat in einem Beschluss aus dem Jahre 2015 die Tätigkeiten von Dolmetschern, Übersetzern und Sachverständigen daher wie folgt präzisiert:<sup>13</sup>

„**Dolmetscher** im Sinne des Prozessrechts (§ 185 GVG) ist ein Sprachkundiger, der zur mündlichen Verhandlung unter Beteiligung von Personen, die der deutschen Sprache nicht mächtig sind, zugezogen wird. Seine Aufgabe besteht darin, den **Prozessverkehr** des Gerichts mit den der Gerichtssprache unkundigen anderen Prozessbeteiligten durch Übertragung der schriftlichen oder mündlich zum Prozess abgegebenen Erklärungen zu ermöglichen [...]. Auch die mündliche Übertragung von Tonbandmitschnitten, die in einer Hauptverhandlung vorgespielt werden, ist eine Dolmetscherleistung. [...]“

„Ein **Übersetzer** ist ein Sprachmittler, der fixierten Text von einer Ausgangssprache in eine Zielsprache übersetzt [...]. Dabei ist die Ausgangsform (gesprochenes Wort, Tonträger- oder Telekommunikationsaufzeichnung oder Textform) unerheblich [...]. Übersetzer i. S. v. § 11 JVEG ist, wer **schriftlich** von einer in eine

andere Sprache überträgt [...]“ „Anders als Dolmetscher und Übersetzer hat der **Sprachsachverständige** die Aufgabe, einen zu dolmetschenden oder zu übersetzenden Text zu **interpretieren** [...], insbesondere bei Erläuterung von im Ausgangstext vorkommenden Abkürzungen, bei unklaren Begriffen, bei unvollständigem oder unklarem Ausgangstext, bei erforderlichen rechtsvergleichenden Überlegungen, aber auch bei Auslegung anderssprachiger Sprachbilder und Redewendungen [...]“

#### 2. Europäische Vorgaben und ihre Umsetzung

Mit Blick auf das EU-Recht gehören die bereits in deutsches Recht umgesetzten EU-Richtlinien 2010/64/EU<sup>14</sup> und 2012/13/EU<sup>15</sup> zu den neueren rechtlichen Rahmenbedingungen, die die Tätigkeit von Übersetzern und Dolmetschern besonders beeinflussen. Diese Normen zielten darauf ab, der Justiz qualifizierte Dolmetscher zur Verfügung zu stellen und die Zusammenarbeit von Justiz und Dolmetschern, insbesondere im Strafverfahren, zu verbessern (u.a. durch Weiterbildungen von an Strafverfahren beteiligten Richtern, Staatsanwälten und Justizbediensteten). Nach *Kotzurek* wurden die Qualitätsansprüche der Richtlinie aber nur teilweise erreicht.<sup>16</sup>

#### 3. Übersetzungsverständnis im Recht – Der Mythos der Wörtlichkeit

Das falsch verstandene Primat der Wörtlichkeit ist aus meiner Sicht eines der größten Probleme im Zusammenhang mit der Fremdwahrnehmung der Translation im Rechtsbereich und der Rolle, die Dolmetschern und Übersetzern rechtlich zugeschrieben wird. In der juristischen Literatur und Rechtsprechung herrscht häufig noch die Meinung vor, dass der Dolmetscher wie ein „Übersetzungsautomat“ wörtlich zu übertragen habe, ohne jegliche Interpretation, so auch im Karlsruher Kommentar zur StPO:

„**Wörtlich zu übersetzen** [sic] sind prozesserhebliche Erklärungen, Anklagesatz, Anträge, Entscheidungen.“<sup>17</sup>

Es ist verständlich, dass Gerichte einen möglichst unverstellten Zugang zu den Aussagen in der Ausgangssprache haben müssen. Sie sehen in der Interpretation beim Dolmetschen die Gefahr, dass ihre Rolle bei der Gesetzesauslegung und Rechtsanwendung beeinträchtigt wird. Die Interpretation durch den Dolmetscher wird im Münchner Kommentar zur StPO daher einerseits als möglicher „Verlust“ gewertet:

„Das Gericht hat kraft § 244 Abs. 2 StPO darüber zu wachen, dass im Rahmen der **Übersetzungstätigkeit** [sic] keine wesentlichen Informationen (durch die „Interpretation“ von Einlassungen und Zeugenaussagen) verloren gehen.“<sup>18</sup>

Andererseits werden laut Münchner Kommentar zur StPO auch Rechtskenntnisse des Dolmetschers als negativ wahrgenommen:

„Eine über die Fachtermini hinausgehende Kenntnis vom materiellen Recht wird vom Dolmetscher nicht erwartet, was im Hinblick auf dessen besondere Verantwortung zwar kritisch zu sehen, aber der zugeschriebenen Rolle als „reiner Übersetzer“ [sic] auch immanent ist. Gerade juristisches Hintergrundwissen kann als „gefährliches Halbwissen“ die Übersetzungsqualität [sic] beeinträchtigen.“<sup>19</sup>

Doch Übersetzen und Dolmetschen ist eben keine einfache und mechanische Ersetzung von sprachlichen Elementen einer Sprache durch Elemente einer anderen Sprache. Die meisten sprachlichen Ausdrücke haben vielschichtige Bedeutungen und Konnotationen, die je nach fachlichem Kontext und Kulturkreis stark variieren können. Auch diese Erkenntnis greift der Münchner Kommentar zur StPO inzwischen mit Verweis auf *Kranjčić*<sup>20</sup> auf:

„Es ist bekannt, dass das Bild des Dolmetschers als Übersetzungsmaschine – gerade aus der Perspektive der Strafverfolgung – dem Idealtypus entspricht, translationswissenschaftlich jedoch an der Realität vorbeigeht. Zwar kann man – anknüpfend an ein bestimmtes Bild von der Rolle des Dolmetschers – die Maßstäbe an die Übersetzungstätigkeit [sic] in die eine oder andere Richtung justieren, Regeln für das „interpretieren“ und „sinngemäße Übersetzen“ aufstellen bzw. Grundsätze für die Reichweite von Textäquivalenz benennen. Dies ändert allerdings nichts daran, dass deren Einhaltung der Kontrolle der Prozessbeteiligten weitestgehend entzogen ist.“<sup>21</sup>

Es ist nicht möglich zu kommunizieren, ohne zu interpretieren, also ohne zwischen verschiedenen Bedeutungsebenen und kulturspezifischen Ausdrucksformen zu entscheiden. Die Absurdität des Primats der wörtlichen Wiedergabe lässt sich z. B. an Redewendungen, ironischen Aussagen oder falschen Freunden illustrieren. Ein weiteres grundlegendes Missverständnis besteht darin, dass nicht einzelne Wörter übersetzt werden, sondern (mündliche oder schriftliche) Texte, die in einem bestimmten Kontext stehen. Gerade das Dolmetschen ist eine Leistung, die **stark situationsgebunden** ist, da sie stets in einem spezifischen kommunikativen und kulturellen Kontext stattfindet. Wenn z. B. das Wort „Erinnerung“ ausgesprochen wird, muss der Dolmetscher aufgrund der Polysemie dieses sprachlichen Ausdrucks entscheiden, ob es sich um eine Gedächtnisleistung, eine Mahnung oder einen Rechtsbehelf handelt. Diese Entscheidung kann nur in einem kommunikativen und situativen Zusammenhang und mit dem entsprechenden Vorwissen gefällt werden.

*Kranjčić*<sup>22</sup> kommt auch zum Ergebnis, dass die „Wörtlichkeit [...] für ein Translat, das zu kommunikativen Zwecken eingesetzt wird, nicht geeignet“ ist. Zur Illustration führt er ein Beispiel aus einem Gerichtsverfahren an, in dem ein Angeklagter aus einem anglophonen afrikanischen Staat als unglaublich eingestuft wurde, weil er seinen Mitangeklagten fälschlicherweise als Bruder bezeichnet habe. Im Nachhinein stellte sich heraus, dass es in seinem Kultur-

kreis durchaus üblich ist, Personen derselben ethnischen Gruppe oder auch bloß Personen mit freundlicher Gesinnung als „brother“ zu bezeichnen. Durch die wörtliche Verdolmetschung als „Bruder“ sei ein Missverständnis entstanden, das für den Betroffenen von großem Nachteil gewesen sei.<sup>23</sup>

#### 4. Spezifische Herausforderungen im Zusammenhang mit Dolmetschen

Obwohl insbesondere das Dolmetschen im Strafverfahren von großer praktischer Relevanz sei, fehlt es laut *Kranjčić* bislang an einer angemessenen Auseinandersetzung mit den damit einhergehenden Konsequenzen und Problemen: „Die einschlägigen übersetzungswissenschaftlichen Erkenntnisse der letzten Jahrzehnte wurden von Rechtswissenschaft und juristischer Praxis weitgehend ignoriert“.<sup>24</sup> Das bestätigt sich auch in der erwähnten Entscheidung des OLG Schleswig von 2015, die lediglich Wikipedia-Einträge als Quellen zitiert, aber keine translologische Literatur.<sup>25</sup> Zutreffend bemerkt *Kranjčić* ferner, dass selbst die Eidesformel in §189 (1) GVG „**daß er [der Dolmetscher] treu und gewissenhaft übertragen werde**“ keine Klarheit über die Rolle und die Tätigkeit von Dolmetschern schaffe, weil die Treue juristisch nicht definiert sei. „Während sich die **Gewissenhaftigkeit** auf die Arbeitsweise des Dolmetschers bezieht [...], bezieht sich das Erfordernis der ‚**Treue**‘ auf den Gegenstand der Übertragung. [...] Wann [...] eine Übertragung treu ist, darüber schweigt sich das Gesetz aus. Auch in der einschlägigen Literatur findet sich kein Hinweis darauf, was dieser Eid im Einzelnen bedeuten soll.“<sup>26</sup>

Obwohl viele Verfahren ohne Sprachmittlung gar nicht durchgeführt werden könnten, empfinden manche Gerichte die Mitwirkung des Dolmetschers immer noch als störend, weil dadurch die gewohnte unmittelbare Kommunikation mit den Prozessbeteiligten verstellt werde. Außerdem nehmen Gerichtsverhandlungen mit Dolmetscher mehr Zeit in Anspruch und können eine höhere Geräuschkulisse verursachen. Andererseits wissen die Gerichte, dass sie auf die Verdolmetschung angewiesen sind, ggf. auch auf „Erläuterungen kultureller Aspekte, damit das Verständnis und die Würdigung einer Aussage durch das Gericht überhaupt möglich werden“.<sup>27</sup> In diesen Fällen handelt der Dolmetscher dann tatsächlich in der Rolle als Sprach- oder Kultursachverständiger. Als Beispiel sei hier der Fall eines Entlastungszeugen aus Ex-Jugoslawien genannt, der aufgrund seiner Bestätigung, dass der Mitarbeiter die Tat nicht begangen haben kann, wegen Meineids verurteilt wurde: „Wir sind Silvester nach Jugoslawien gefahren, haben Weihnachten dort unten verbracht und sind pünkt-

lich am Neujahrsmorgen zurückgewesen“.<sup>28</sup> Staatsanwaltschaft und Gericht hielten den Zeugen für unglaublich, obwohl dieser auf der Richtigkeit seiner Informationen beharrte. Die Lösung: Sie waren an „Silvester am 31.12. in Deutschland losgefahren, [hatten] Weihnachten, nämlich das orthodoxe Weihnachtsfest am 6., 7. und 8. Januar zu Hause verbracht, und [waren] pünktlich am Neujahrsmorgen, das in Ostserbien nach julianischem Kalender am 14. Januar liegt, wieder zurück in Deutschland“.<sup>29</sup>

Um die Komplexität der Tätigkeit von Dolmetschern zu illustrieren, wird hier noch eine Entscheidung des OLG Saarbrücken herangezogen, die in einer Beschreibung der notwendigen Fähigkeiten von Gerichtsdolmetschern unter anderem aufzählt:<sup>30</sup>

„Auch wer zwei Sprachen perfekt in Wort und Schrift beherrscht, wird durch diese Fähigkeiten noch nicht notwendigerweise zum Dolmetscher und Übersetzer qualifiziert. Die Ausübung dieser Tätigkeit in der zu fordernden Qualität erfordert vielmehr über die bloße Sprachkompetenz hinaus, dass der Bewerber zusätzlich u. a. über die Fähigkeiten verfügt [...]: Gewandtheit im Ausdruck; Fähigkeit der Anpassung an den jeweiligen Text und seine Sprachform; rasche Auffassungsgabe; gutes Gedächtnis; Konzentrationsfähigkeit und Einfühlungsvermögen; **die Befähigung, mögliche Missverständnisse und Fehldeutungen der Übertragung vorzusehen und bei der Wiedergabe auszuschalten**; [...].“

Die genannte Befähigung, mögliche Missverständnisse und Fehldeutungen [...] auszuschalten, erfordert ein kritisches Mitdenken und die Interpretation im kommunikativen Kontext.

#### IV. Verbesserung der Zusammenarbeit

Nach dieser Übersicht der verschiedenen Auffassungen zur Translation im Allgemeinen und im Rechtsbereich im Besonderen kommen wir nun zurück zu der Ausgangsfrage: Wie können Vertreter der juristischen Berufe und Sprachmittler besser zusammenarbeiten?

Aus meiner Sicht sollten sich beide Berufsgruppen eingehender mit Inhalten und Feinheiten der Tätigkeiten der jeweils anderen Berufsgruppe beschäftigen und im Berufsalltag an einem Strang ziehen, um gemeinsam dem Interesse der Wahrheitsfindung und der Wahrung der Rechte von Beschuldigten oder Antragstellern, die der deutschen Sprache nicht mächtig sind, gerecht zu werden. Damit Dolmetscher und Übersetzer ihren Beitrag leisten können, sind berufliche Wertschätzung und Vertrauen, aber auch Fachwissen über diese Tätigkeit erforderlich, denn:

„Als **Hilfsorgan** der Entscheidungsträger trägt er [der Dolmetscher und Übersetzer] dazu bei, die ebenfalls im Rechtsstaatsprinzip verwurzelte Garantie eines fairen Verfahrens sicherzustellen.“<sup>31</sup>

Dolmetscher sind nach herrschender Meinung zwar Gehilfen des Gerichts,<sup>32</sup> sie können aber nach einer Entscheidung des OLG Hamburg aus dem Jahr 2018 durchaus auch als Organe der Rechtspflege eingestuft werden:

„Mitglieder des Gerichts, der Staatsanwaltschaft und Verteidiger als Organe der Rechtspflege – **auch Dolmetscher werden hierzu zu rechnen sein** – haben eine Prozessberichterstattung mit Foto- und Filmaufnahmen ihrer Person grundsätzlich hinzunehmen.“<sup>33</sup>

Denn:

„In seiner Rolle als Mittler zwischen Verfahrensbeteiligten leistet der Dolmetscher und Übersetzer einen **unentbehrlichen Beitrag zur Gewährleistung des Rechts auf rechtliches Gehör**, das ein wesentliches Element des Rechtsstaatsprinzips darstellt.“<sup>34</sup>

Diese Rolle zu stärken, sollte im ureigenen Interesse von Justiz und Behörden liegen. Die Justiz ist hier besonders gefragt, weil sie für die Beeidigung zuständig ist, aber auch die Justizministerien sollten Weiterbildungen i.S.d. Art. 6 der Richtlinie 2010/64/EU anbieten und das betreffende Personal regelmäßig schulen. Hierbei könnten drei grundlegende Aspekte im Vordergrund stehen.

#### 1. Vorbereitung von Dolmetschern

Wie bereits erwähnt, ist das Dolmetschen eine stark situationsgebundene Leistung. Aus diesem Grund ist eine umfassende inhaltliche und terminologische Vorbereitung auf Dolmetscheinsätze erforderlich. Was bei professionellen Dolmetschern trotz erheblichen Zeitdrucks scheinbar mühelos aussieht, ist in Wahrheit ein sehr komplexer und anstrengender kognitiv-intellektueller Vorgang.

Die Qualität der Dolmetschleistung steht in direktem Zusammenhang mit der Qualität der Vorbereitung. So wie sich Richter, Staatsanwälte und Rechtsanwälte auf Gerichtsverhandlungen vorbereiten, benötigen auch Dolmetscher Akteneinsicht und/oder Informationen für die Vorbereitung eines professionellen Dolmetscheinsatzes, insbesondere bei komplexeren Verfahren, in denen z. B. Sachverständigengutachten verlesen werden. Es gilt die Grundregel: **Ein guter Dolmetscher ist ein vorbereiteter Dolmetscher** (oder umgekehrt: **Ein vorbereiteter Dolmetscher ist ein guter Dolmetscher**). Es gibt durchaus Gerichte, die Verständnis für die Notwendigkeit der (zweisprachigen!) inhaltlichen und terminologischen Einarbeitung in komplexere Sachverhalte erkennen und den Dolmetschern nicht nur Vorbereitungs-material zur Verfügung stellen, sondern auch ihre Vorbereitungszeit vergüten.<sup>35</sup> Auch die ISO-Norm 20228:2019 zum juristischen Dolmetschen sieht dies vor:

„Judicial and other authorities as well as clients in general are encouraged to provide legal interpreters access to case-related

and other reference materials in order to enable them to prepare for the interpreting service.”<sup>36</sup>

Gerichte sollten Dolmetschern vorab zumindest relevante Informationen über das Verfahren zur Verfügung stellen, in welchem sie die Gerichte unterstützen sollen. Die Realität sieht vielmehr so aus, dass dem Dolmetscher häufig keinerlei Informationen gegeben werden mit der Begründung, er müsste ja „**nur übersetzen** [sic]“ und weil alle Informationen dem Datenschutz unterliegen. Allgemein beeidigte Dolmetscher sind aber nach § 189 Abs. 4 GVG ohnehin gehalten, Verschwiegenheit zu wahren („[...]Der Dolmetscher oder Übersetzer **soll** [...] Verschwiegenheit wahren), wobei in einzelnen Ländergesetzen, wie z.B. in Sachsen, diese Pflicht noch präziser formuliert ist: „[...] dem Sprachmittler **ist es untersagt**, Tatsachen, die ihr oder ihm bei der Ausübung ihrer oder seiner Tätigkeit zur Kenntnis gelangen, Dritten unbefugt mitzuteilen oder sie zum Nachteil anderer zu verwerten“.<sup>37</sup> Außerdem sind professionelle Dolmetscher meistens in Berufsverbänden mit einem verpflichtenden Berufsethos organisiert, das u.a. den streng vertraulichen Umgang mit Informationen aus den von ihnen bearbeiteten Aufträgen vorsieht.<sup>38</sup> Gerichte wären gut beraten, häufiger einen kritischen Blick darauf zu werfen, **warum** bestimmte Dolmetscher, die über Agenturen entsandt werden, nicht beeidigt sind. In den meisten Fällen liegt es daran, dass sie nicht qualifiziert sind und daher auch nicht in Berufsverbänden aufgenommen wurden.

Manchmal argumentieren Gerichte auch, dass Dolmetschern die Einsichtnahme in die Verfahrensakten nur deshalb verwehrt wird, damit sie „unvoreingenommen“ und unparteilich dolmetschen. Hier wird manchmal fälschlicherweise eine Analogie zur Tätigkeit von Schöffen hergestellt. All das kann nicht im Interesse der Justiz und anderer Institutionen, die auf gute Dolmetschqualität angewiesen sind, sein.

## 2. Qualifikation und Translationsmodi

Die Justiz könnte noch viel mehr von professionellen Dolmetschleistungen profitieren, wenn sie enger mit qualifizierten Dolmetschern zusammenarbeiten würde. Zudem sollten Gerichte beeidigte Sprachmittler möglichst direkt beauftragen und *Ad-hoc*-Beeidigungen auf Ausnahmefälle beschränken (z. B. Dringlichkeit, selten vertretene Sprachen usw.). Außerdem sollte die von der Justiz geführte und aktuell gehaltene Dolmetscherdatenbank (<[www.justiz-dolmetscher.de](http://www.justiz-dolmetscher.de)>) besser bekanntgemacht werden, um die zwar bequemere, aber problematische Beauftragung über Agenturen zu vermeiden. Wenn über Agenturen geladen wird, sollte die Justiz zumindest strenger darauf achten, dass diese allgemein beeidigte Dolmetscher entsenden.

Auch wenn die Berufung auf den allgemein geleisteten Eid aus rechtlicher Sicht der *Ad-hoc*-Beeidigung gleichgestellt ist, scheint der Unterschied im Hinblick auf die Qualifikation des Dolmetschers nicht ausreichend bekannt zu sein.

Außerdem wäre es hilfreich, wenn Juristen „übersetzen“ und „dolmetschen“ terminologisch sauber unterscheiden würden, da es nicht nur wissenschaftlich gesehen erhebliche Unterschiede zwischen diesen Translationsmodi bestehen, sondern auch im Recht, was sowohl die Definitionen des OLG Schleswig in seiner Entscheidung aus dem Jahr 2015 als auch die unterschiedliche Vergütung von Übersetzern, Dolmetschern und Sachverständigen<sup>39</sup> im JVEG belegen. Vor diesem Hintergrund muss der Beschluss des Bundesgerichtshofs aus dem Jahr 2017 zur Hinzuziehung eines Dolmetschers in gerichtlichen Verhandlungen als negatives Beispiel gesehen werden. Dort verwenden die obersten Bundesrichter 24 Ausdrücke zum Übersetzen (Übersetzungsleistung, Übersetzer, simultane Übersetzung, Übersetzen in der Hauptverhandlung usw.) und 15 Ausdrücke zum Dolmetschen (Dolmetscher, Dolmetscherleistung, Dolmetschertätigkeit, Hinzuziehung eines Dolmetschers), obwohl es in der gesamten Entscheidung ausschließlich um das Dolmetschen geht.<sup>40</sup>

## 3. Gute Praktiken

Eine gute Praxis hat sich in einem 2015 durchgeführten Großverfahren vor dem Landgericht Nürnberg-Fürth bewährt.<sup>41</sup> In diesem Verfahren mit neun Angeklagten (von denen sechs eine Verdolmetschung ins Englische, zwei in Yoruba benötigten) und über 60 Verhandlungstagen hatte sich der Vorsitzende Richter der Kammer von einer professionellen Dolmetscherin beraten lassen und mit ihr zusammen die folgenden Rahmenbedingungen abgesteckt:<sup>42</sup> Die organisierende Dolmetscherin stellte eine Gruppe von qualifizierten Dolmetschern (alle beeidigt, mit Erfahrung im Simultan- und im Gerichtsdolmetschen) zusammen, die per Sammelladung beauftragt wurden. Sie koordinierten die Einsätze untereinander, sodass sich das Gericht nicht mehr darum kümmern musste. An jedem Prozesstag standen zwei qualifizierte und vorbereitete Dolmetscher zur Verfügung. Zudem wurde die Terminologie zentral auf einem Server verwaltet. Das für Dolmetscher und Angeklagte sehr anstrengende und für das Gericht durch die Geräuschkulisse störende Flüsterdolmetschen<sup>43</sup> wurde vermieden und durch eine kostengünstige technische Lösung ersetzt. Die Dolmetscher hatten sich mit einer „mobilen Flüsteranlage“ (Personenführungsanlage) an einer für die Akustik und den Sichtkontakt günstigen Stelle des Raumes platziert. Diese Anlage besteht aus kleinen, ansteckbaren Sendern, einem



Ansteckmikrofon und Empfängergeräten. Die Dolmetscher sprechen sehr leise ins Mikrofon, die Angeklagten hören die Verdolmetschung über die Empfängergeräte, in die wiederum entweder Einohr-, Kinnbügel- oder Überkopfhörer eingesteckt werden, wobei die Zuhörer die Lautstärke selbst regulieren können. Da die Dolmetscher ihre Sender an der Kleidung mit dem Ansteckclip befestigt hatten, konnten sie bei akustischen Schwierigkeiten trotzdem aufstehen und sich im Gerichtssaal an die Stelle begeben, an der sie am besten hören [und ggf. sehen] konnten. Die Dolmetscher wechselten sich ab, wie beim Kabinensimultandolmetschen ebenfalls üblich, und waren daher auch noch am Nachmittag eines langen Sitzungstages leistungsfähig. Dieses Setting kann als Vorbild für eine gute Zusammenarbeit zwischen Gerichten und Dolmetschern dienen.

Auch die in Art. 6 der Richtlinie 2010/64/EU geforderten, aber offensichtlich nicht systematisch stattfindenden Weiterbildungen von an Strafverfahren beteiligten Richtern, Staatsanwälten und Justizbediensteten zu den Besonderheiten einer dolmetschergestützten Verständigung könnten z. B. durch Erproben eines solchen Szenarios durchgeführt werden, auch in einfacheren Konstellationen in kleineren Gerichtsverfahren.

## V. Schlussbemerkungen

Juristen, Übersetzer und Dolmetscher haben gemein, dass sie die Sprache als wichtiges Arbeitsinstrument verwenden. Trotzdem könnte der Austausch zwischen diesen Berufsgruppen deutlich verbessert werden, wenn Juristen mehr über das Dolmetschen und Übersetzen wüssten und Übersetzer und Dolmetscher mehr über die rechtliche Stellung und Funktion von Übersetzern, Dolmetschern und Sachverständigen. Die gelungene professionelle Zusammenarbeit zwischen Dolmetschern und dem Landgericht Nürnberg-Fürth kann ein Vorbild sein und auch in kleiner dimensionierten Gerichtsverfahren zur Nachahmung einladen. Die Justiz hat ein intrinsisches Interesse an hoher Dolmetschqualität und kann davon nur profitieren, da eine mangelhafte Verdolmetschung oder unethisches Verhalten von unqualifizierten Dolmetschern zu Berufungen oder Revisionen führen können.

Das in Art. 6 der Richtlinie 2010/64/EU formulierte Ziel, in Weiterbildungen von an Strafverfahren beteiligten Richtern, Staatsanwälten und Justizbediensteten auf die Besonderheiten einer dolmetschergestützten Verständigung einzugehen, sollte weiterhin diejenigen antreiben, welche die Relevanz von hoher Dolmetschqualität im Rechtswesen erkennen.

1 Gesetz über die allgemeine Beeidigung von gerichtlichen Dolmetschern (Gerichtsdolmetschergesetz – GDolmG) <<https://www.gesetze-im-internet.de/gdolmg/BJNR212400019.html>> (Zugriff: 2.5.2025).

2 T. Reichmann, „Welche juristischen Inhalte für die Dolmetscheraus- bildung?“, *Babel* 66 (2020), S. 311–325.

3 S. Monjean-Decaudin, *Traité de juritraductologie. Épistémologie et méthodologie de la traduction juridique*, 2022.

4 T. Reichmann, „Ein translatologischer Blick auf die Fachsprache des Rechts oder ein rechtlicher Blick auf die Translatologie – Brauchen wir eine neue Disziplin?“, in: M. Adams/K. Baumann/H. Kalverkämper (Hrsg.), *Zukunftsformate der Fachkommunikations- forschung*, 2023, S. 259–277.

5 S. Monjean-Decaudin/ J. Popineau-Lauvray, „How to apply comparative law to legal translation. A new juritraductological approach to the translation of legal texts“, in: L. Biel/J. Engberg/M. Martín/ R. Ruano Rosario/V. Sosoni (eds.), *Research methods in legal translation and interpreting*. 2019, S. 115–129.

6 O. Kade, „Zufall und Gesetzmäßigkeit der Übersetzung“, in: Beihefte zur Zeitschrift Fremdsprachen 1. Leipzig 1968, S. 35.

7 O. Kade, aaO.

8 E. Prunč, *Entwicklungslinien der Translationswissenschaft*, 2012, S. 16.

9 E. Felder/F. Vogel, *Sprache im Recht*, 2022.

10 Zu nennen sind hier insbesondere für das Privatrecht das Max-Planck-Institut für ausländisches und internationales Privatrecht und für das Strafrecht (v.a. im Hinblick auf die Übersetzungen ausländischer Strafgesetzbücher) das Max-Planck-Institut für ausländisches und internationales Strafrecht [jetzt Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht].

### Prof. Dr. Tinka Reichmann

Universität Leipzig – Institut für Angewandte Linguistik und Translatologie



11 Ich danke Frau Christiane Schmitt, Vorsitzende Richterin am LG Saarbrücken und Direktorin des Amtsgerichts Saarlouis, und Herrn Dr. Sigurd Wern, Vorsitzender Richter am LG Saarbrücken, für wertvolle Hinweise auf die Rechtsprechung.

12 BGH, Urteil vom 28.11.1950 (2 StR 50/50), Hervorhebungen durch die Autorin.

13 OLG Schleswig, Beschluss vom 23.03.2015 – 1 Ws 79/15, BeckRS 2015, 11001. Hervorhebungen durch die Autorin.

14 Richtlinie 2010/64/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über das Recht auf Dolmetschleistungen und Übersetzungen in Strafverfahren, ABl. L 280 vom 26.10.2010, 1.

15 Richtlinie 2012/13/EU des Europäischen Parlaments und des Rates vom 22. Mai 2012 über das Recht auf Belehrung und Unterrichtung in Strafverfahren, ABl. L 142 vom 1.6.2012, 1.

16 M. Kotzurek, „Die Richtlinie 2010/64/EU zum Dolmetschen und Übersetzen in Strafverfahren: Neues Qualitätssiegel oder verpasste Chance? Zur Umsetzung in Deutschland, Polen und Spanien“, *eucri* 2020, 314 – 321. Siehe auch verschiedene Beiträge der „European



Legal Interpreters and Translators Association", (EULITA) unter <https://www.eulita.eu/en/> (Zugriff: 2.5.2025).

17 KK-StPO/Diemer, 9. Aufl. 2023, GVG § 185, Rn. 3, 4.

18 MüKoStPO/Oğlakcioğlu, 1. Aufl. 2018, GVG § 185 Rn. 70–71, Hervorhebungen durch Autorin.

19 MüKoStPO/Oğlakcioğlu, GVG § 185 Rn. 22–23, Hervorhebungen durch Autorin.

20 C. Kranjčić, „... dass er treu und gewissenhaft übertragen werde.“: Zum Dolmetschen im Strafverfahren, 2010.

21 MüKoStPO/Oğlakcioğlu, GVG § 185 Rn. 10–11, Hervorhebungen durch Autorin.

22 C. Kranjčić, „... dass er treu und gewissenhaft übertragen werde.“: Zum Dolmetschen im Strafverfahren, 2010, S. 214.

23 C. Kranjčić, Dolmetschen im Strafverfahren: wider die Wörtlichkeit und für wirkliche Zweckorientierung (oder: Wem dient der Dolmetscher?), NSTZ 2011, 658.

24 C. Kranjčić, Dolmetschen im Strafverfahren: wider die Wörtlichkeit und für wirkliche Zweckorientierung (oder: Wem dient der Dolmetscher?), NSTZ 2011, 657f.

25 Siehe OLG Schleswig, Beschluss vom 23.03.2015 – 1 Ws 79/15, BeckRS 2015, 11001, Rn. 10, 11.

26 C. Kranjčić, „... dass er treu und gewissenhaft übertragen werde.“: Zum Dolmetschen im Strafverfahren, 2010, S. 42, Hervorhebungen durch Autorin.

27 C. Kranjčić, „... dass er treu und gewissenhaft übertragen werde.“: Zum Dolmetschen im Strafverfahren, 2010, S. 54.

28 D. Gradinčević-Savić, „Aus dem Erfahrungsschatz einer Justizdolmetscherin“, FORUM online 2/2019, Dezember 2019, Hattingen: Aticom, S. 6.

29 D. Gradinčević-Savić, „Aus dem Erfahrungsschatz einer Justizdolmetscherin“, FORUM online 2/2019, Dezember 2019, Hattingen: Aticom, S. 6–7.

30 OLG Saarbrücken, Beschluss vom 25.04.2005 (1 VA 1/05), Hervorhebungen durch Autorin.

31 M. Ronellenfitch/R. Dorn, *Rechtsfragen des Vergütungsanspruchs von Dolmetschern und Übersetzern nach dem Justizver-*

*gütungs- und -entschädigungsgesetz (JVEG)* [Gutachten], 2006, [https://bb.bdue.de/fileadmin/files/PDF/Gut\\_zu\\_wissen/fragen\\_gutachten\\_14\\_jveg.pdf](https://bb.bdue.de/fileadmin/files/PDF/Gut_zu_wissen/fragen_gutachten_14_jveg.pdf) (Zugriff: 2.5.2025), S. 32.

32 OLG Koblenz, Urteil vom 22.03.2017 – 1 OLG 4 Ss 201/16.

33 OLG Hamburg, Beschluss vom 12.09.2018 – 1 WS 71/18.

34 M. Ronellenfitch/R. Dorn, *Rechtsfragen des Vergütungsanspruchs von Dolmetschern und Übersetzern nach dem Justizvergütungs- und -entschädigungsgesetz (JVEG)* [Gutachten], 2006, S. 32.

35 Mündliche Auskunft von Frau Christiane Schmitt, seinerzeit Vorsitzende Richterin der Wirtschaftsstrafkammer am Landgericht Saarbrücken, seit 1.1.2022 Direktorin des Amtsgerichts Saarlouis.

36 M. Ronellenfitch/R. Dorn, a.a.O.

37 §11 Sächsisches Dolmetschergesetz, <https://www.revosax.sachsen.de/vorschrift/19920-Saechsisches-Dolmetschergesetz> (Zugriff: 2.5.2025).

38 Berufs- und Ehrenordnung des BDÜ: <https://bdue.de/der-bdue/statuten/berufs-und-ehrenordnung>.

39 Sprachsachverständige werden im JVEG genauso wie andere Sachverständige vergütet.

40 BGH, Beschluss vom 08.08.2017 (1 StR 671/16).

41 Landgericht Nürnberg-Fürth, Az. 13 KLs 804 Js 22059/13. In der Entscheidung werden aber weder die Sprachen noch die technische Dolmetschlösung erwähnt.

42 M. Flaszynski/E. Limberger-Katsumi, „Dolmetschen bei Großprozessen: Mehr Effizienz und bessere Arbeitsbedingungen“, *MDÜ* 6/2016, 26–29.

43 Das Flüsterdolmetschen (auch *Chuchotage*, aus dem Französischen *chuchoter* für flüstern) ist eine Variante des Simultandolmetschens: Der Dolmetscher oder die Dolmetscherin sitzt hierbei allerdings nicht versteckt in einer schalldichten Kabine, sondern direkt neben dem Zuhörer. Beinahe zeitgleich zum Gesagten spricht der Flüsterdolmetscher oder die Flüsterdolmetscherin mit gedämpfter Stimme die Übersetzung für den neben ihm sitzenden Teilnehmer und kann auf diese Weise für maximal zwei Personen dolmetschen (<https://aiic.de/leistungen/flueterdolmetscher/>).

# Imprint

## Impressum

Published by:

**Max Planck Society for the Advancement of Science**  
**c/o Max Planck Institute for the Study of Crime, Security and Law**

(formerly Max Planck Institute for Foreign and International Criminal Law), represented by Director Prof. Dr. Ralf Poscher

Guenterstalstrasse 73  
79100 Freiburg i.Br., Germany

Tel: +49 (0)761 7081-0  
E-mail: [public-law@csl.mpg.de](mailto:public-law@csl.mpg.de)

Internet: <https://csl.mpg.de>

Official Registration Number: VR 13378 Nz  
(Amtsgericht Berlin Charlottenburg)  
VAT Number: DE 129517720



**Editor in Chief:** Prof. Dr. Dr. h.c. mult. Ulrich Sieber

**Managing Editor:** Thomas Wahl, Max Planck Institute for the Study of Crime, Security and Law, Freiburg

**Editors:** Dr. Anna Pinggen, Max Planck Institute for the Study of Crime, Security and Law, Freiburg; Cornelia Riehle, ERA, Trier

**Editorial Board:** Prof. Dr. Lorena Bachmaier, Complutense University Madrid, Spain; Prof. Dr. Esther Herlin-Karnell, University of Gothenburg, Sweden; Dr. Fabio Giuffrida, Team Leader, DG Justice and Consumers, European Commission; Mirjana Juric, Head of Service for combating irregularities and fraud, Ministry of Finance, Croatia; Philippe de Koster, Director FIU Belgium; Prof. Dr. Katalin Ligeti, University of Luxembourg; Dr. Lothar Kuhl, Former Head of Unit, European Commission (Anti-Fraud Office (OLAF) and Directorate for Audit in Cohesion (DAC)); Prof. Dr. Ralf Poscher, Director at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg, Germany; Lorenzo Salazar, Deputy Prosecutor General to the Court of Appeal of Naples (ret.), Italy; Prof. Rosaria Sicurella, University of Catania, Italy

**Language Consultants:** Indira Tie and Sarah Norman, Certified Translators, Max Planck Institute for the Study of Crime, Security and Law, Freiburg

**Typeset and Layout:** Ines Hofmann and Katharina John, Max Planck Institute for the Study of Crime, Security and Law, Freiburg

**Produced in Cooperation with:** Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)

**Printed by:** Stücker Druck und Verlag, Ettenheim, Germany

The publication is co-financed by the  
Union Anti-Fraud Programme (UAFP),  
managed by the European Anti-Fraud  
Office (OLAF)



Co-funded by  
the European Union

© Max Planck Institute for the Study of Crime, Security and Law, 2025. This journal is published Open Access under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. For details, see <https://creativecommons.org/licenses/by-nd/4.0/>.

Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ISSN: 1862-6947

### Practical Information

Articles in eucrim are subject to an editorial review. The journal is published four times per year and distributed electronically for free. Articles can be published in English, French and German.

In order to receive issues of the periodical on a regular basis, please write an e-mail to:

[eucrim-subscribe@csl.mpg.de](mailto:eucrim-subscribe@csl.mpg.de)

For cancellations of the subscription, please write an e-mail to:

[eucrim-unsubscribe@csl.mpg.de](mailto:eucrim-unsubscribe@csl.mpg.de)

More information at our website: <https://eucrim.eu>

### Contact

Thomas Wahl

Max Planck Institute for the Study of Crime, Security and Law  
Guenterstalstrasse 73

79100 Freiburg i.Br., Germany

Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)

E-mail: [info@eucrim.eu](mailto:info@eucrim.eu)



**MAX PLANCK INSTITUTE**  
FOR THE STUDY OF  
CRIME, SECURITY AND LAW

