eucrim
2026 / 1
European Law Forum: Prevention • Investigation • Prosecution

20 06–2026 years of eucrim

Procedural Safeguards
Garanties procédurales
Verfahrensgarantien

Editorial: "20 Years of eucrim" by *Ulrich Sieber*

Guest Editorial for this Issue by *Sirpa Rautio*

Julia Laffranque: OLAF's Controller of Procedural Guarantees in the Twilight Zone between Procedural Fairness and Investigative Effectiveness

Anže Erbežnik: EU Procedural Rights Directives and their CJEU Evolution

Katalin Ligeti: Reinforcing EU Core Values in Criminal Justice

Salvador Guerrero Palomares: Justice Systems Built on Confidence

Vânia Costa Ramos, Amedeo Barletta and Elise Martin-Vignerte: Towards a New Roadmap for Defence Rights

Lorena Bachmaier Winter: Rethinking Procedural Safeguards in the Digital Age

2026 / 1 ISSUE / ÉDITION / AUSGABE

eucrim 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://eucrim.eu/associations/.

Contents

News

European Union

Foundations

5 Rule of Law
8 Area of Freedom, Security and Justice
9 Schengen
11 Ukraine conflict
15 Artificial Intelligence
16 Digital Space Regulation
16 Legislation

Institutions

17 European Parliament
17 Court of Justice of the European Union
18 OLAF
21 European Public Prosecutor's Office
24 Anti-Money Laundering Authority
26 Europol
27 Eurojust
28 Frontex

Areas of Crime

29 Protection of Financial Interests
34 Tax Evasion
36 Corruption
38 Money Laundering
42 Environmental Crime
43 Cybercrime
45 Organised Crime
46 Terrorism

Procedural Law

48 Procedural Safeguards
50 Data Protection
53 Freezing of Assets / Confiscation

Council of Europe

Cooperation

54 Police Cooperation
55 Judicial Cooperation
55 European Arrest Warrant
58 Transfer of Sentenced Persons

Foundations

60 Human Rights Issues

Institutions

61 European Committee on Crime Problems

Areas of crime

62 Corruption
63 Money Laundering
65 Counterfeiting & Piracy

Articles

Procedural Safeguards

66 Fil Rouge by *Katalin Ligeti*

67 OLAF's Controller of Procedural Guarantees in the Twilight Zone between Procedural Fairness and Investigative Effectiveness
Julia Laffranque

75 EU Procedural Rights Directives and their CJEU Evolution
Anže Erbežnik

85 Reinforcing EU Core Values in Criminal Justice – Insights from the HighLevel Forum on the Future of EU Criminal Justice
Katalin Ligeti

95 Justice Systems Built on Confidence – The CCBE Proposal on the Future of EU Criminal Justice
Salvador Guerrero Palomares

105 Towards a New Roadmap for Defence Rights – The ECBA's Vision for the Future of EU Criminal Justice
Vânia Costa Ramos, Amedeo Barletta and Elise Martin-Vignerte

112 Rethinking Procedural Safeguards in the Digital Age – Bulk Surveillance, Artificial Intelligence, and the Need for Responses at the EU Level
Lorena Bachmaier Winter

Editorial: 20 Years of eucrim

The first issue of *eucrim* was published in September 2006. With the present issue, *eucrim* celebrates a 20-year success story. This anniversary provides an opportunity to look back, take stock, and look ahead.

I.

The history of *eucrim* is closely linked to the protection of the European Communities' financial interests in the early 1990s. The growing budgets of the Communities led to a significant rise in fraud. In particular, the spectacular "Greek maize" case in the late 1980s showed that some Member States had little interest in prosecuting these offences against the Community at the *national level*, particularly since any losses uncovered were charged to the respective Member States. The creation of criminal law at the *supranational level* was blocked by the governments of the states in the Council. National courts were also sceptical. The German Federal Constitutional Court, for example, unlike the European Court of Justice later on, rejected the idea of the EC having ancillary competence in criminal matters. It grounded its reasoning, above all, in the close links between criminal law and national culture, as well as in the necessary democratic legitimacy underpinning criminal law.

To remedy this unsatisfactory state of affairs, from the late 1980s onwards, the European Commission pursued a wise policy, focusing heavily on European civil society and fostering direct contacts with the staff in national administrations responsible for the allocation of European funds: It funded studies by legal scholars, training courses for national practitioners, and activities by civil society associations campaigning for more effective sanctions legislation and better protection of the Communities' financial interests. The key initiators of this network of associations were *Francesco de Angelis* from the European Commission's Directorate-General for Financial Control, *Dr h.c. Diemut Theato* as Chair of the Committee on Budgetary Control in the European Parliament, and *Lothar Kuhl* from the anti-fraud body UCLAF/OLAF, all of whom rendered outstanding services in this regard.

In collaboration with national partners, a network of 32 European Lawyers' Associations was established within a short space of time across 30 European countries. These Associations cooperated closely with one another and organised joint seminars and studies on European criminal law and the protection of the European Union's financial interests. During the Associations' heyday, hardly a month went by without a major seminar, attended by numerous representatives from all Member States and the European Union. From 1993 to 2002, the exchange of information between the Associations was supported by the bulletin *Agon*, which was a precursor to *eucrim*. This collaboration within the Associations proved to be extremely unifying and productive. For instance, at that time, I was not only President of the German Association for European Criminal Law, but also a special adviser to two Commissioners; my professional contacts within the Association, including regular collaboration with representatives of German authorities, also allowed access to files held by the German Customs Investigation Bureau, which proved to be a treasure trove of ideas for reform proposals aimed at combating subsidy fraud.

Ulrich Sieber

These activities of the associations and the broader context in which they took place gave rise to important new ideas concerning the development of European criminal law and the protection of the EU's financial interests. These included, in particular, the idea of a European Public Prosecutor's Office within the *Corpus Juris*, the principle of mutual recognition of judicial decisions, the expansion of severe administrative sanctions as a substitute for the EU's lack of criminal law competence, and the increased incorporation of non-criminal preventive measures. The working group set up by the European Commission to develop the Corpus Juris was chaired by the President of the French Association for European Criminal Law Research, *Prof. Dr Mireille Delmas-Marty*, and most members of this

group, as well as the research group tasked with the follow-up study also came from the European Lawyers' Associations. As a result, these Associations became a strong counterbalance to national voices resisting the Europeanisation of criminal law, which argued that criminal law was deeply rooted in "national culture". Given the lack of information amongst many European legal scholars and practitioners at that time, the advocates of more extensive Europeanisation did not have it easy.

II.

In this context, from 2004 onwards, I developed the concept for *eucrim* at the Max Planck Institute for Foreign and International Criminal Law, together with the head of my unit for European criminal law, *Thomas Wahl*. The intention of this project has been to raise awareness and to improve knowledge of the Europeanisation of criminal and "criministrative" law. The impetus for this initiative was the criticism – often unfounded – of emerging European criminal law voiced at the extraordinary criminal law scholars' conference on European criminal law held in Dresden, Germany, in 2003. The discussion at this conference highlighted the need for better information on current European developments and prompted me to spontaneously announce the launch of a newsletter dedicated to this purpose.

The primary aim of *eucrim* was, and remains, to provide a fact-based, systematically organised, and concise summary of news and events relating to European criminal law and the protection of European financial interests: The news items in *eucrim* contain links that direct the reader to the respective source documents, thereby creating an objective basis for information and discussion. Additional "Spotlights" (visually highlighted) provide more detailed coverage of particularly important developments. The articles in the journal, usually revolving around a focal topic, complement this news reporting and, crucially, enable a critical discussion of the issues at hand.

From the very conception of *eucrim*, the use of information technology was a central concern of mine in achieving this objective. Consequently, from the outset, the journal was not only distributed in print but also made available online free of charge (Diamond Open Access). In addition, each issue is promoted through an email newsletter (to which users can subscribe) that summarises the most important contents and provides practical information.

A significant leap forward in digitalisation took place in 2018 with the redesign of the *eucrim* website, technically implemented by *Thomas Breitner* from the IT-department of the Max Planck Institute. The website's new features now also allow direct online access to *individual* contents of the *eucrim* issues – such as the specific news, articles, and events. This enables individual items to be published on the website as pre-prints immediately after editing and proofreading – making them publicly available in advance of the quarterly issue's finalisation. As a result, *eucrim* now offers a much more up-to-date and more valuable service to its users: This is particularly important when contributions relate to current developments, e.g., in the case of legal policy statements. Users can opt to receive automatically immediate notifications of new website content via a news feed – integrable with email clients like Outlook – whenever new content is published on the website (see "Staying Up-to-Date" in the *eucrim* website footer). In addition, the *eucrim* editorial team uses social media (particularly LinkedIn) to share important content – such as the "Spotlights", pre-prints of articles, news, and the publication of the journal itself.

As a further tool, databases have also been set up for relevant CJEU proceedings and for ratifications of relevant Council of Europe conventions. In the future, digitalisation will be taken even further: A specific AI chatbot has been developed that accesses all published *eucrim* content, providing a reliable and more independent basis for research into European criminal law and the protection of the EU´s financial interests. It will be launched during this anniversary year.

Thanks to these developments, *eucrim*'s impact and reach is now considerable: since its foundation, *eucrim* has published a total of 72 issues containing 368 articles by 393 authors. Since 2018, 2715 news items have been published online. The printed edition of *eucrim* is sent to over 680 individuals, institutions, and libraries worldwide. The email newsletter currently has more than 2100 subscribers. Visits to the *eucrim* website have grown steadily since the 2018 revamp, reaching 328,000 visits in 2025. Individual *eucrim* items have also achieved considerable reach. Notably, *Drago Kos's article* on 'War and Corruption in Ukraine' (*eucrim* 2022, Issue 2) has been accessed 11,505 times since publication. Among the news, the *Spotlight* on the EU's anti-money laundering package has been viewed over 14,500 times to date. In addition, statistics on the users indicate that *eucrim* is intensively read not only across Europe but also in countries outside Europe, such as the USA.

To achieve these goals and results, an entire team is behind the editorial and technical success of *eucrim*, with each member responsible for a specific area. These include, first and foremost, the members of the Editorial Board listed on

the *eucrim* homepage. At its annual meetings, the Board provides guidance on the focus of upcoming issues and supports the acquisition of articles, often in collaboration with staff from OLAF and other European institutions. Subject-matter editors are responsible for identifying, analysing, and summarising the news. They include *eucrim*'s Managing Editor, *Thomas Wahl*, *Cornelia Riehle,* and *Dr Anna Pingen*, along with *Prof. Els de Busser* and *Dr András Csúri,* who have contributed in the past.

The indispensable support of other staff members at the Max Planck Institute in Freiburg also contributes to *eucrim*'s achievements – particularly in the areas of IT, language editing, typesetting and design, public relations, distribution, budget management, and accounting. Financial support from the EU's Anti-Fraud Programme, administered by OLAF, and from the Department of Public Law at the Max Planck Institute for the Study of Crime, Security and Law in Freiburg, headed by *Prof. Dr Ralf Poscher*, is also key to the success of *eucrim*. I would like to take this opportunity to express my sincere thanks to them all!

III.

Perhaps the most important reason for *eucrim*'s present and future progress, alongside the outstanding commitment in terms of personnel and technology, is its thematic and content-based concept. This is primarily characterised by its broad international, interdisciplinary, and cross-regime orientation, which must continue to shape and drive European criminal policy – now and in the future. Four catalysts have emerged to propel this initiative:

- First, the comprehensive integration of Europe's various national legal systems, supranational EU law, and the law of the Council of Europe have long been underway. Eucrim takes equal account of the approaches adopted by both small and large Member States, from which best practices and key insights emerge. This broad perspective fosters the development of new, innovative models of cooperation and responses.
- Secondly, close cooperation between academia and legal practice is central to eucrim. This foundational principle also stems from the activities of the European Criminal Law Associations. In eucrim, the convergence of academia and legal practice is evident not only in the contributions of individual authors but also in the composition of the Editorial Board, which includes leading European legal scholars and practitioners.
- Thirdly, for *eucrim*'s continued success, it is important to devote space to alternative legal regimes and non-legal preventive measures, because the protection of European values cannot be achieved through criminal law alone. Their protection must also take into account *other legal regimes*, such as administrative law, administrative *penal* law, money laundering law, confiscation law, and civil law. *Non-legal* means, such as technical or organisational measures, are also highly relevant.
- Fourthly, particularly when developing such alternative systems, the protection of civil liberties – generally well-established in traditional criminal law in Europe – must be incorporated and taken into consideration from the outset. Criminal law safeguards can provide important impetus for the other legal regimes in this regard.

The focal topics that *eucrim* features on its website (under "issues") demonstrate that the journal is very much committed to the protection of human rights and to the aforementioned international, interdisciplinary, and cross-regime approach. This is also evident from the four focal topics for the 2026 anniversary year, which cover important pillars of European criminal law and the protection of the EU´s financial interests: procedural safeguards (Issue 1/2026), the harmonisation of substantive criminal law (Issue 2/2026), the law on cooperation (Issue 3/2026), and the relevant supranational institutions (Issue 4/2026).

IV.

This illustrates: *Eucrim* continues to be a timely, high-calibre, and highly influential information platform and forum for discussion on European criminal law and security law, as well as the protection of the European Union's financial interests. It transcends the scope of a traditional journal by far.

The *eucrim* concept can therefore also serve as a reference point for strengthening the justification of European approaches in other key policy areas – such as European defence and economic policy. The current geopolitical challenges in Ukraine, in the Middle East, and in the USA, as well as the rise of anti-European right-wing parties in Europe, make *eucrim*'s European approach more important than ever for the future.

In this spirit, *eucrim* will place even greater future emphasis on how the prevention and prosecution of European crime and the protection of European financial interests can be improved through close cooperation between EU institutions, Member States, and civil society. Contributions on this topic are welcome!

Professor Dr Dr h.c. mult. Ulrich Sieber, *eucrim* Editor-in-Chief, Director Emeritus at the Max Planck Institute in Freiburg

Guest Editorial for this Issue

Dear Readers,

Looking back at the last 20 years, the European Union has taken substantial strides towards establishing a specific legal framework to ensure the rights of defendants in criminal proceedings – as set out in its secondary law, underpinned by the EU Charter of Fundamental Rights. In parallel, the rights of crime victims – long given secondary consideration – have been strengthened across Member States in accordance with EU law, for example, in the newly revised Victims' Rights Directive.

While there have been welcome achievements, it remains crucial that the EU continues its efforts to ensure the effective implementation of procedural safeguards in line with the relevant case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

The EU Agency for Fundamental Rights (FRA) has been supporting EU institutions and Member States on this implementation journey, regularly emphasising that Member States are obliged to protect these rights. In practice, we are seeing that they do not necessarily apply them in the same way. This can weaken trust between national judicial authorities, as well as with the general population, and interfere with cooperation in matters relating to the EU's area of freedom, security and justice – and, more broadly, the rule of law. Simply formally transposing EU legislative instruments into national law is not sufficient; they must be made effective in practice.

We are witnessing how rising concerns about terrorism, cybercrime, and hybrid threats often trigger calls for exceptional measures. Some argue that certain safeguards could hinder the ability to address such threats. However, procedural safeguards should not be viewed as obstacles to security but instead as prerequisites for legitimate and effective criminal justice and sustainable security responses. Security policies must be founded on our values, ensuring that the principles of necessity, proportionality and legality remain at the heart of responses to security threats. Appropriate safeguards must be in place to guarantee accountability and provide for judicial redress. In today's climate of polarisation and misinformation, procedural fairness is more important than ever – not only for guaranteeing justice in individual cases, but also for strengthening public confidence and for serving as a democratic stabiliser.

Sirpa Rautio

The increasing digitalisation of justice and the use of new technologies, such as AI, raise questions about whether a digital rendering of defence rights can be considered equivalent to the original concept. Rather than being merely technologically efficient, the EU owes its citizens an agile digital criminal justice response based on a "rights-by-design" approach, with oversight frameworks in place. This was one of the conclusions of the High-Level Forum on the Future of EU Criminal Justice, in which FRA participated. There is a need for continued examination of updates to the procedural rights acquis in light of technological developments, including AI-generated/produced evidence, as noted in FRA's reports on "Digitalising Justice" and "Assessing high-risk AI".

As the EU considers measures to make future EU law more responsive to emerging threats, it is important to keep the full spectrum of fundamental rights in mind. All future measures in this area must be evidence-based, to ensure that we effectively close any gaps between the law on paper and the law in action, including critical assessments of shortcomings. FRA will continue to underpin this endeavour with its research, which is based on the experiences of hundreds of legal practitioners, alongside the experiences of defendants, offenders, witnesses, and victims. FRA's research findings can help support the EU and its Member States in developing effective criminal justice responses in order to better address crime and its newly arising challenges in the years to come.

Sirpa Rautio, Director of the EU Agency for Fundamental Rights (FRA)

News

Actualités / Kurzmeldungen

European Union

Reported by Thomas Wahl (TW), Cornelia Riehle (CR), Dr. Anna Pingen (AP), and Joscha Kanstinger (JK)

Foundations

Rule of Law

Hungary: Rule-of-Law Developments January–August 2026

This news item provides an update on relevant rule-of-law developments in Hungary that have implications for Union law, particularly with regard to the protection of the EU's financial interests. The reporting period is from 1 January to mid-August 2026. The period is characterised by the landslide victory of *Péter Magyar's* Tisza party in the 12 April 2026 parliamentary elections, leading to expectations in Europe that Hungary will rebuild its rule-of-law standards following *Viktor Orbán's* 16-year tenure. This is a precondition for the release of billions of euros of EU funding that has been blocked. This overview builds on the one in eucrim 3/2025, pp. 188–191.

■ **27 January 2026:** The Grand Chamber of the European Court of Justice rules in Case C-271/23 that Hungary failed to fulfil its obligations under EU law by voting against the Council's common position regarding the rescheduling of Cannabis at a session of the United Nations Commission on Narcotic Drugs. The ECJ finds that, under Art. 3(2) TFEU, the Union has exclusive external competence where international measures may affect common Union rules or alter their scope. This is the case with regard to the term „drugs" as defined in Council Framework Decision 2004/757/JHA laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking. According to the Court, by voting, within an international body, against a common position of the Council, Hungary compromised the principle of sincere cooperation as well as the principle of unity in the international representation of the EU and its Member States.

■ **9 February 2026:** The Hungarian Helsinki Committee (HHC) publishes a brief outlining on how the „state of danger" rules continue to be a powerful tool in the hands of the executive and undermine the separation of powers. The HHC points out that recent constitutional amendments to the rules of the „state of danger", such as the formal requirement of parliamentary authorisation to override Acts of Parliament, do not limit government power in practice, given that the current Government holds a stable two-thirds majority in the Parliament. Furthermore, the amendments leave intact the most problematic features of the legal framework, including an excessive carte blanche mandate for the Governement.

■ **10 February 2026:** According to the annual Corruption Perceptions Index (CPI) compiled by the Secretariat of Transparency International in Berlin, Hungary remains the most corrupt EU country for the fourth consecutive year. Hungary shares the last place with Bulgaria this time, but it is the lowest record of Hungary in the CPI. The poor result reflects the continued failure to remedy rule of law deficiencies and to curb systemic corruption, according to the report.

■ **12 February 2026**: In her opinion on Case C-829/24, Advocate General (AG) *Juliane Kokott* calls on the ECJ to rule that Hungary has failed to fulfil its obligations under EU law in several respects by adopting the Protection of National Sovereignty Act. Adopted on 12 December 2023, the Act established, *inter alia*, a new authority, the "Sovereignty Protection Office" (SPO). It was officially tasked with "protecting constitutional identity" and was granted extensive powers and discretion to conduct investigations against individuals or legal entities that are

* Unless stated otherwise, the news items in the following sections cover the period 16 January 2026 – 15 June 2026. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

suspected of serving foreign interests or threatening national sovereignty (→eucrim 4/2023, 311). In the AG's view, the SPO's powers of investigation and disclosure together with the corresponding obligations to cooperate, are indirectly discriminatory and Hungary infringed several fundamental freedoms, as specified by the „Services" Directive. The AG also finds that the threat of an investigation and of its findings being published in accusatory or stigmatising reports, and the risk of criminal proceedings, have a chilling effect and may lead to self-censorship by journalists and/or publishers and press organisations. This infringes the freedom of expression and information guaranteed by the CFR. Other provisions of the Act interfere with the freedom of association and the professional secrecy between lawyers and clients. Lastly, the processing of personal data by the SPO does not comply with the GDPR and the CFR.

■ **26 February 2026:** The Grand Chamber of the European Court of Justice rules in Case C-92/23 that Hungary infringed the freedom of expression and information by refusing to renew the broadcasting licence of the radio station „Klubrádió". The case initially arose from an automatic rejection due to formal omissions in reporting obligations, and subsequently from the non-acceptance of the application under a new tender procedure. The judges in Luxembourg emphasise that the allocation of frequencies must be carried out strictly in accordance with objective, transparent, non-discriminatory and proportionate criteria. An automatic rejection, even in the case of minor breaches of obligations that have since been rectified, is disproportionate. The Court also emphasised that, given the central role of audiovisual media in shaping public opinion, radio frequencies constitute a crucial means of access to freedom of broadcasting and the media. Restrictions on access to these frequencies therefore directly interfere with this fundamental right and require particularly stringent justification.

■ **12 April 2026:** The Tisza Party, led by MEP *Péter Magyar*, wins the parliamentary elections in Hungary, defeating the incumbent Fidesz-KDNP government of Prime Minister *Viktor Orbán*. The Tisza Party wins 141 of the 199 parliamentary seats, corresponding to more than two-thirds. This „supermajority" allows the party to amend Hungary's constitution (Fundamental Law) and key laws. With 79% of the electorate voting, this is the highest turnout in any election since Hungary's transition to democracy in 1990. *Viktor Orbán* concedes his defeat after having been 16 years in power. *Péter Magyar* says: „Today was a celebration of democracy. Together we have replaced the Orbán system, together we liberated Hungary and we took back our country". Commission President *Ursula von der Leyen* commented: „Hungary has chosen Europe. Europe has always chosen Hungary. A country reclaims its European path. The Union grows stronger […] Europe's heart is beating stronger in Hungary tonight."

■ **13 April 2026:** *Péter Magyar* holds his first press conference after wining the parliamentary elections. He sets out an ambitious reform programme and gives his views on the European Union, the rule of law, the central bank, and pride/LGBTQ+ rights. He announces that his government „will do everything to restore the rule of law, plural democracy, and the system of checks and balances", without using anti-democratic measures. He pleads for „a strong Central Europe within a strong EU." He also calls on high-level officials who owe their mandate Orban's Fidesz Party, including incumbent Hungarian President *Tamás Sulyok*, to resign or leave office.

■ **21 April 2026:** The Court of Justice of the European Union, sitting as the Full Court, rules that Hungary's so-called "Anti-Paedophilia Act" of 2021 was contrary to EU law. For the first time, the ECJ finds a breach of the fundamental values enshrined in Art. 2 TEU. The ruling in Case C-769/22 concerned infringement proceedings brought by the Commission against Hungary. The Hungarian law prohibits or restricts the portrayal of homosexuality and transgender identities to minors, for example in schools, the media and advertising (→eucrim 2/2021, 72). The ECJ finds that these provisions infringed EU law in several respects. In particular, they affect provisions of internal market law relating to services, as well as the GDPR. The ECJ also finds breaches of the Charter of Fundamental Rights (in particular human dignity, non-discrimination, and freedom of expression and information). Examining a separate infringement of Art. 2 TEU, which lists the values on which the Union is founded and which are common to all the Member States, the Court notes that the aspects of the Act „constitutes a coordinated series of discriminatory measures which are in breach, in a way that is both manifest and particularly serious, of the rights of non-cisgender persons – including transgender persons – or non-heterosexual persons, as well as the values of respect for human dignity, equality and respect for human rights, including the rights of persons belonging to minorities." Thus, for the first time, the Court directly classifies a national law as a breach of the fundamental values of EU law themselves. In doing so, it awards a binding nature to Art. 2 TEU being a justiciable standard, creating a further lever in the enforcement of infringement proceedings and enabling the EU to respond to illiberal developments in Member States. However – as the Court qualifies restrictively – „only manifest and particularly serious breaches of one or more values common to the Member States may give rise to a finding that there has been a failure by a Member State to

fulfil legally binding obligations under Art. 2 TEU, such breaches being incompatible with the very identity of the Union as a common legal order of a society in which pluralism prevails." With its ruling, the Court follows the proposals set out in the Opinion of Advocate General *Ćapeta* of 5 June 2025 (→eucrim 3/2025, 190).

■ **1 May 2026:** Hungarian civil society organisations publish the „Hungarian Citizen Election Report 2026". The report documents systemic abuses and shortcomings observed during the parliamentary election campaign period. Particular attention is drawn to disinformation, social media manipulation, and attempts at foreign interference. The report also offers recommendations aimed at making future elections more transparent and fair. It is emphasised that Hungary still lacks a legal framework for formal civil election observation — a deficiency that weakens trust in the electoral process.

■ **9 May 2026 (Europe Day):** The National Assembly convenes and inaugurates *Péter Magyar* as new Prime Minister of Hungary. He promises a „change of system" after new revelation and allegations of corruption against the former ruling Fidesz party have come to light. Ministers of the new government tell media outlets that those guilty of financial crimes will be held accountable and a new „office to recover stolen assets" will be set up.

■ **25 May 2026:** In an article on *Verfassungsblog*, Professors *John Morijn* and *Kim Lane Scheppele* stress that restoring the rule of law cannot take place in a short space of time and that unfreezing EU funds is impossible without „insisting that EU law must be respected so that EU monies will only be released if and when laws are on the books that are actually being applied". The authors point out that elections that bring about pro-democratic change can be influential to the rule-of-law conditionality, but lessons must be learned from Poland, where the Commission acted too speedily to unfreeze funds after Poland's 2023 election.

■ **26 May 2026:** Following the change of government, the Hungarian delegation provides an update on the current status of the ongoing proceedings under Art. 7(1) TEU concerning the state of the rule of law in the country. At the General Affairs Council meeting, the delegation signals its willingness to cooperate closely with the EU to restore standards of the rule of law. Another aim is to secure the release of EU funds amounting to around €10.4 billion that have so far been blocked.

■ **29 May 2026:** Commission President *Ursula von der Leyen* meets new Hungarian Prime Minister *Péter Magyar*. *Von der Leyen* emphasises that, with the elections of 12 April 2026, „the Hungarian people chose democracy. They chose to return to the heart of our Union". The Commission and Hungary will concentrate on four issues in order to restore the rule of law: (1) Structural reforms, which are much needed to fight corruption and state capture in Hungary; (2) investments for the revised NextGenerationEU plan; (3) progress on the super milestones with regard to Cohesion funds; (4) protection of fundamental rights, notably academic freedom. Von der Leyen announced that €10 billion from the RRF and €6.4 billion in Cohesion Fund can be unlocked for Hungary, provided that the necessary reforms are implemented.

■ **2 June 2026:** In a contribution on European Law Blog, Legal Advisor *Gábor Spuller* analyses the reform process in Hungary initiated by new Prime Minister *Péter Magyar* and his new Minister of Justice, *Márta Görög*. He concludes that the Commission would make an error by unblocking EU funds if it measures only whether violations stop, rather than whether institutional independence is being rebuilt on transparent, accountable foundations.

■ **4 June 2026:** Having filed charges against the organisers of the Budapest and Pécs Pride marches in February, the prosecution services drop the charges. This brings to an end the legal dispute that began when the government of *Viktor Orbán* cracked down on public demonstrations related to LGBTQI issues in 2025. Human rights organisations welcome the step as a restoration of the fundamental right to freedom of assembly.

■ **15 June 2026:** Following Prime Minister *Péter Magyar's* announcement on election night that high public office-holders would be replaced in accordance with rule-of-law standards, the HHC publishes a background paper outlining the criteria that, based on international and EU law, must be taken into account for such replacements. The paper also details the specific legal solutions regarding the three most relevant public offices for rebuilding the rule of law: the President of the Republic, the President of the Kúria and the Constitutional Court Justices.

■ **16 June 2026:** As part of the Article 7(1) TEU procedure, the General Affairs Council receives an update on the current situation regarding the rule of law in Hungary. The Hungarian delegation provides an update on their plans and the concrete steps they are taking to address the concerns raised in the reasoned proposal, the subsequent interim reports by the European Parliament, and the concerns raised by Member States during numerous hearings held at previous Council meetings. The Commission also informs ministers of the progress of discussions with Hungary regarding the three conditionality tracks and the related reforms and remedial actions. A decision to close the procedure is not taken.

■ **23 June 2026:** Following the change of government in Hungary, the Visegrad Group is being revitalised. For the first time in over two years, the heads of state and government of Hungary, Poland, the Czech Republic and Slovakia met again in Gödöllő (Hungary). In their joint statement, they mark the

35th anniversary of the signing of the Visegrad Declaration and reaffirmed the Visegrad Group as a key platform for regional dialogue and cooperation. The countries intend to coordinate their positions more effectively ahead of EU summits in future and to cooperate more closely on issues such as the next long-term EU budget (safeguarding cohesion and agricultural funding), migration, and industrial competitiveness.

■ **10 July 2026:** The Commission adopts a decision confirming Hungary's participation in the European Public Prosecutor's Office (EPPO) →eucrim news of 17 July 2026 with more details. This is a historic step as the new Hungarian government reverses the steadfast refusal to join the independent EU anti-fraud body by the previous *Orbán* administration.

■ **13 July 2026:** The Hungarian National Assembly enacts the 17th amendment to the Fundamental Law. Being conceived as a transitional legislative package designed to dismantle Orbán-era institutional setups, the amendments include, *inter alia*: instant termination of the mandate of the President of the Republic (*Tamás Sulyok*); reintroduction of a 70-year age limit for Constitutional Court (CC) justices resulting in the termination of the mandates of four justices as of 1 September 2026; restoration of the CC's full thematic jurisdiction and its right to elect its own president; reduction of the length of the mandates of various public officeholders; introduction of new rules governing the election and termination of the mandates of judicial leaders; limitation of the mandates of members of Parliament to three terms (12 years); reduction of the number of laws requiring a two-thirds majority for adoption; and establishment of a new authority tasked with the recovery and protection of state assets (see also above).

■ **17 July 2026:** The Commission releases its 2026 Rule of Law Report. In the country chapter on Hungary, the Commission acknowledges that the new Hungarian government „has engaged in intense reform efforts to restore the rule of law". The report positively highlights Hungary's decision of May 2026 to join the EPPO (see above) and progress made in anti-corruption measures, asset declarations and the work of the Integrity Authority. Despite progess in several areas, the Commission sees continuing shortcomings that must be addressed by Hungary. An example is the low rate of prosecutions and final judgments for high-level corruption cases.

■ **11 August 2026:** Based on the 17th amendment to the Fundamental Law (see above), *András Barka* is elected as the new President of Hungary. While the opposition Fidesz and KDNP parliamentary groups boycotted the election, Barka received 140 votes from members of Parliament, counting on the two-thirds majority of the ruling Tisza party. As a renowned legal scholar, Barka was also a judge at both the ECtHR and Hungary's Supreme Court. His election renews hopes that the new president will support *Peter Magyar's* government in its efforts to restore the rule of law in Hungary. (TW)

Area of Freedom, Security and Justice

2026 EU Justice Scoreboard

spot light

On 4 June 2026, the European Commission published the 2026 EU Justice Scoreboard, the fourteenth edition of its annual comparative overview of the efficiency, quality, and independence of the justice systems of all 27 Member States. As in earlier years (for the 2025 Scoreboard →eucrim 2/2025, 118–119), the Scoreboard did not establish an overall ranking but assembled indicators meant to support national reforms and mutual learning. It feeds into the Annual Rule of Law Cycle and the Commission's Rule of Law Report, into the European Semester, and into the closing phase of the Recovery and Resilience Facility. Much of the quantitative data was again supplied by the European Commission for the Efficiency of Justice (CEPEJ) and covers the years 2014 to 2024.

Building on the single-market orientation introduced in 2025, the 2026 edition adds and refines indicators on independent authorities regarded as relevant for the internal market – among them supreme audit institutions, national competition authorities, first-instance public procurement review bodies, and preventive anti-corruption bodies. It also presents new figures, including on accessibility for persons with disabilities, the powers of equality bodies, child-friendly proceedings, the digitalisation of justice, and the transparency of lobbying. The key developments outlined in the 2026 Scoreboard are:

■ **Efficiency:** The figures show broadly positive trends in civil, commercial, and administrative cases, with efficiency back to 2019 levels after a dip recorded in 2020 to 2021. Of particular relevance for criminal justice practitioners, the Scoreboard again measures the length of first-instance proceedings in money-laundering and bribery cases. In money-laundering matters, first-instance proceedings lasted on average between one month and one year in twelve Member States; between one and two years in ten Member States; and more than three years in three Member States. In bribery cases, proceedings were concluded within about a year in six Member States; between one and two years in ten Member States; and two years or more in four Member States for which data were available.

■ **Quality:** The quality of justice systems covers aspects of accessibility, human and financial resources and digitalisation. As in the previous year's Scoreboard, people whose income is

below the Eurostat poverty threshold cannot receive legal aid in three Member States. There is also a high disparity between Member States regarding the rate of legal aid paid to criminal defence lawyers in a specific criminal case. All Member States have some specific arrangements for child-friendly justice and proceedings, for both civil and criminal/juvenile justice proceedings. 11 Member States have all nine of the monitored specific arrangements in place, including measures to separate children from adults if they are deprived of their liberty. Significant differences persist between Member States in spending on law courts, both per inhabitant and as a percentage of GDP. On digitalisation, the Scoreboard finds significant room for improvement. With regard to online information on judicial systems, the situation remains stable compared to 2025, but some differences still exist between Member States as regards information and the degree to which it responds to people's needs. For example, only nine Member States employ chatbots to help the public find information about the justice system. Figures also show that the potential of the use of digital technology by courts and prosecution services can be higher. Although there has been steady overall progress in digital-ready procedural rules, only six Member States allow fully for the use of distance communication and for the admissibility of evidence in digital format only.

- **Independence:** Drawing on Eurobarometer surveys of the general public (FL581) and of companies (FL582), the perceived judicial independence has improved or remained stable compared with 2016 in twenty Member States among the public, and in eighteen Member States among companies. Interference or pressure from government and politicians remains the reason most often cited for a perceived lack of independence, followed by pressure from economic interests. The 2026 edition also introduces and updates structural indicators on probationary periods for judges, on the management powers of Prosecutors General, on the allocation of cases within prosecution offices (developed with the NADAL Network), and on the independence of bars and lawyers.
- **Anti-corruption:** Specifically on anti-corruption, next to new and updated figures on the length of judicial proceedings in bribery cases (see above), the 2026 Scoreboard maps national transparency registers, which help prevent corruption by ensuring transparent lobbying. Data show that 16 Member States have such a register in place, presenting an overview of how they work, and which officials are subject to transparency requirements in their interactions with lobbyists.

The 2026 Justice Scoreboard concludes that it has further developed an in-depth insight into the effectiveness of justice systems in the Member States. *Michael McGrath*, Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection stressed that the Scoreboard „is an essential tool for strengthening justice systems and upholding the rule of law across the Union". (AP/TW)

EU-India Strategic Agenda

At the 16th EU-India Summit, which took place on 27 January 2026 in New Delhi, the EU and India agreed on a comprehensive strategic agenda that aims to further reinforce their partnership in several areas by 2030. The agenda includes commitments to a number of projects designed to significantly deepen and broaden cooperation between the two partners in the fields of justice and home affairs in the coming years. These projects include:

- Implementation of the EU-India Security and Defence Partnership (SDP), covering maritime security, cyber and hybrid threats, space and counter-terrorism;
- Conclusion of an EU-India Security of Information Agreement to facilitate the exchange of classified information and ensure stronger security and defence cooperation;
- Enhanced exchanges on hybrid threats and sharing of best practices in this area;
- Strengthened law enforcement cooperation through the implementation of the Working Arrangement between the Indian Central Bureau of Investigation (CBI) and Europol;
- Planned cooperation between relevant Indian authorities and Eurojust and the European Public Prosecutor's Office;
- Enhanced cooperation to dismantle illicit drug production and improve coordination to prevent drug trafficking.

A priority for the strengthened law enforcement cooperation will be countering terrorism. This cooperation will particularly cover countering radicalisation and violent extremism, combatting the financing of terrorism, promoting internationally agreed anti-money laundering standards, preventing the exploitation of new and emerging technologies for terrorist purposes, and tackling terrorist recruitment. (TW)

Schengen

ECJ Clarifies Scope of SIS Rules on Surrender of Seized Objects

On 4 June 2026, the ECJ ruled in Case C-326/25 (*CY v 03 Rayonno upravlenie na SDVR*) on the scope of Regulation 2018/1862 concerning alerts in the Schengen Information System (SIS) for objects sought for seizure or use as evidence in criminal proceedings. For the new legal framework on the SIS →eucrim 4/2018, 192–193.

➤ *Background of the case*

The case concerned a vehicle registered in Bulgaria that was stopped during a police check. The Bulgarian authorities found that the vehicle's chassis number matched an alert en-

tered in the SIS by Germany and the temporary Head of the 3rd District Police Department at the Sofia Directorate for Internal Affairs, Bulgaria. The alert concerned a vehicle sought for use as evidence in criminal proceedings.

Following the hit, the Bulgarian authorities seized the vehicle and contacted the German SIRENE Bureau. The German authorities stated that the vehicle had been reported in connection with an offence of unlawful appropriation and that the company identified as the rightful owner wished to have it returned. The Bulgarian authorities then ordered the vehicle to be surrendered to a representative of that company.

The person registered as the owner of the vehicle in Bulgaria challenged the surrender order before the Bulgarian courts. He argued, in substance, that he had been excluded from the administrative and judicial procedure concerning the return of the vehicle, even though the measure affected his rights and interests.

The referring *Varhoven administrativen sad* (Supreme Administrative Court, Bulgaria) is uncertain as to whether the Bulgarian legislation complies with the SIS Regulation when right holders have no participatory rights in the return proceedings.

➤ *The ECJ's ruling*

The ECJ held that Art. 39 of Regulation 2018/1862 lays down the steps to be taken following a hit on an object alert: the executing Member State must seize the object in accordance with national law and contact the issuing Member State in order to agree on the measures to be taken. However, the Regulation does not determine the procedural rules governing a subsequent national decision to surrender or repatriate the object in response to the issuing Member State's request.

Therefore, national rules on the adoption of such a surrender decision do not fall within the scope of Regulation 2018/1862. The definition of procedural rules is entirely up to the national law. Since that national procedure was not considered to constitute the implementation of EU law within the meaning of Art. 51(1) of the Charter, the Charter was not applicable either. Consequently, the ECJ did not answer the separate question concerning effective judicial protection under Art. 47 of the Charter. (AP)

Commission: Internal Border Controls by Nine Member States Should Phase Out

On 2 June 2026, the Commission issued opinions on the temporary reintroduction of internal border controls by nine EU Member States: Austria, Denmark, France, Germany, Italy, The Netherlands, Norway, Slovenia and Sweden. The Commission recommended that the Member States concerned work towards phasing out and gradually lifting internal border controls, making full use of available alternative measures and intensifying regional cooperation. The Commission stressed that, while the situation in each Member State is different, several common key issues could be identified.

It pointed out, *inter alia*, that the upcoming entry into application of the Pact on Migration and Asylum will reinforce the management of the EU's external borders and provide Member States with more effective tools to address unauthorised movements within the Schengen area. The Commission also believes that the new EU information systems – the Entry-Exit System (which has been fully applicable since April 2026) and the future rollout of the European Travel Information and Authorisation System (ETIAS) – will improve oversight of movements across the EU's external borders, and thus support the monitoring of persons entering and leaving the Union and crossing borders. The Commission ultimately calls on EU Member States to increase the use of non-systematic police checks or mobile biometric identification and vehicle tracking technologies as effective alternatives to internal border controls. The Member States should gradually replace border checks with alternative solutions.

According to the Schengen law (the Schengen Borders Code), a Member State can reintroduce internal border controls in view of addressing a serious threat to public policy or internal security, when this is necessary and proportionate. In principle, the maximum duration of border controls at internal borders shall not exceed two years. The Commission is obliged under the Schengen Borders Code to assess the necessity and proportionality of the prolonged internal border checks (over 12 months for the same reason). This has been done now by the opinions. (TW)

German Court Finds German Check at Luxembourg Border Unlawful

On 27 April 2026, the Administrative Court of Koblenz, Germany *(Verwaltungsgericht Koblenz)* ruled that an identity check by the German Federal Police *(Bundespolizei)* at the German–Luxembourg border was unlawful. The judgment is significant because it applies the revised Schengen Borders Code, in particular the amended rules on the temporary reintroduction and prolongation of internal border controls in exceptional situations involving large-scale unauthorised migration movements.

➤ *Background of the case*

The case concerned a German law professor who travelled by bus from Luxembourg to Saarbrücken in June 2025. Shortly after crossing the border at Perl-Schengen, the bus was directed to a rest area on the A8 motorway, where the Federal Police carried out an identity check. The plaintiff challenged the measure, arguing that the internal border controls on which the check was based had been unlawfully prolonged.

Germany had prolonged internal border controls at the border with Luxembourg for the period from 16 March 2025 to 15 September 2025. The Federal Government mainly invoked continued irregular migration, smuggling-related crime, a high number of asylum applications and pending asylum proceedings, pressure on reception and integration systems, and burdens on administrative and security authorities. The plaintiff argued that these reasons did not satisfy the requirements of the Schengen Borders Code and that he was likely to be affected by similar controls again because of frequent professional travel to Luxembourg.

➤ *The Court's decision*

The Administrative Court of Koblenz upheld the action and found that the identity check was unlawful. The relevant provision of the Federal Police Act could not justify internal border controls unless those controls had themselves been lawfully reintroduced or prolonged under EU law. Since internal border controls are generally prohibited under Art. 22 of the Schengen Borders Code, as well as under the EU Treaties, they may only be reintroduced or prolonged under the strict conditions laid down in the Schengen Borders Code.

The Court found that Germany had not sufficiently demonstrated that the conditions for prolonging the controls under Art. 25 of the Schengen Borders Code were met. In particular, the government had failed to establish a sufficiently reliable factual basis showing that a sudden and very high number of unauthorised migration movements was placing significant pressure on the resources and capacities of well-prepared authorities. The Court considered the references to exhausted administrative capacities and public services too vague to allow for a plausibility review. The Court also rejected the argument that a protracted or already declining migration situation could still be treated as "sudden" within the meaning of Art. 25(1) of the Schengen Borders Code.

As a result, the Court held that the prolongation of the internal border controls at the German-Luxembourgish border for the relevant period was contrary to EU law. The identity check carried out against the plaintiff therefore lacked a sufficient legal basis and violated his general freedom of action and right to informational self-determination under German constitutional law. The Court allowed an appeal because the legal requirements for internal border controls under the revised Schengen Borders Code have not yet been clarified by higher courts. (AP)

Entry/Exit System (EES) Fully Operational Since 10 April 2026

Since 10 April 2026, the Entry/Exit System (EES) has been fully operational at all external borders of the Schengen Area. Following the completion of the phased rollout that began in October 2025 (→eucrim 2/2025, 111), the entries and exits of third-country nationals on short stays are now digitally recorded across the EU. Travellers' facial image, fingerprints and personal data from the travel document are also recorded. The previous manual passport stamping is no longer required.

According to a Commission press release of 30 March 2026, more than 45 million border crossings have already been recorded since the system's launch. Over 24,000 people had been refused entry for different reasons.

The goal of the EES is to strengthen control of the EU's external borders, systematically detect overstays, and combat document and identity fraud. In Romania, for instance, authorities recently discovered that an individual was attempting to travel using two different identities and had been denied entry on multiple previous occasions. Without the EES, this case would likely have gone undetected. The system is operated by the EU agency eu-LISA and also forms the technical basis for the European Travel Information and Authorization System (ETIAS), which is scheduled to go live at the end of 2026. (TW)

Ukraine Conflict

Europol Clarifies Role in Data Sharing and SIS Alerts

In response to a media article suggesting that information shared via Europol may have been linked to subsequent security measures (including entry bans) in the Schengen Information System (SIS) concerning former Ukrainian prisoners held in Russian-occupied Ukrainian territories, Europol published a fact check on 20 February 2026: It details the exchange of information between the agency and national law enforcement authorities. Europol pointed out that, while national authorities can use the agency's Secure Information Exchange Network Application (SIENA) to share the personal data of suspects with Europol and each other, Europol itself cannot enter names into the SIS. Although non-EU countries may request Europol to facilitate the entry of so-called „information alerts" into the SIS by EU Member States, this is not yet a possibility due to ongoing technical implementation.

Europol only processes information in SIENA related to criminal activities that fall within its remit. The agency emphasised that national authorities independently decide how to use criminal intelligence shared by partner countries and that EU Member States and non-EU partners, including Ukraine, can exchange operational information via SIENA without Europol's involvement. (CR)

JIT to Focus on Deportation of Ukrainian Children

At the beginning of March 2026, the Joint Investigation Team (JIT) on al-

leged core international crimes in Ukraine, established in March 2022 (→eucrim 1/2024, pp. 8–9), had its mandate extended by another two years. The aim of the JIT is to facilitate investigations and prosecutions in the relevant Member States as well as any measures that may be brought before the ICC. The JIT members from Estonia, Latvia, Lithuania, Poland, Romania, Slovakia, and Ukraine, together with partners Eurojust, Europol, and the Office of the Prosecutor of the International Criminal Court (ICC-OTP), will now focus more strongly on the illegal transfer of Ukrainian children and their deportation to Russia and Belarus. (CR)

EU Reactions to Russian War against Ukraine: Overview March – Mid-June 2026

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 protection of the EU's financial interests, on the EU's internal security policy, and on criminal law.

The following overview covers the period from March 2026 to mid-June 2026. For overviews of developments in previous periods →eucrim 3/2024, 174–176, →eucrim 4/2024, 267–268, →eucrim 1/2025, 6–7, →eucrim 2/2025, 114–118, and →eucrim 4/2025, 255–258, each with further references.

■ **4 March 2026:** The European Commission releases its 2025 General Report, taking stock of the EU's main actions during a year shaped by growing geopolitical instability. The report points in particular to the Union's continued engagement with Ukraine, including financial assistance, humanitarian relief, military support, and restrictive measures against Russia.

■ **6 March 2026:** Justice Commissioner *Michael McGrath* reports to EU Justice Ministers on work to strengthen accountability for crimes committed in and against Ukraine. He underlines the importance of setting up the Special Tribunal for the Crime of Aggression against Ukraine and calls for progress on the International Claims Commission for Ukraine, while also reaffirming the role of the International Criminal Court in prosecuting atrocity crimes.

■ **14 March 2026:** The Council extends the individual sanctions targeting persons and entities responsible for undermining or threatening Ukraine's territorial integrity, sovereignty, and independence for another six months. The measures, now prolonged until 15 September 2026, continue to apply to around 2,600 individuals and entities and include asset freezes, travel restrictions, and a ban on making funds or economic resources available to listed persons and entities.

■ **16 March 2026:** The Council imposes sanctions on nine individuals held responsible for atrocities committed in Bucha and neighbouring areas during the early phase of Russia's full-scale invasion of Ukraine. The listings include senior Russian military officials whose units are linked to killings of civilians, executions, looting, and torture. The Council states that the conduct amounts to war crimes and crimes against humanity.

■ **16 March 2026:** The Council adds four individuals to the EU sanctions list for Russian information manipulation and interference activities. The listings target propagandists and media figures accused of spreading narratives that justify Russia's war of aggression against Ukraine, including calls for further violence, the denial of Ukrainian identity, and disinformation about Ukraine and its armed forces. The measures are adopted under the EU sanctions framework addressing Russia's destabilising hybrid activities against the EU, Ukraine, and other partners.

■ **25 March 2026:** The Commission presents AGILE, a new €115 million funding instrument to speed up defence innovation. The initiative responds to lessons from Russia's war against Ukraine by supporting faster development, testing, and deployment of technologies such as drones, artificial intelligence, and quantum solutions, with a focus on start-ups and SMEs.

■ **26 March 2026:** The ECJ rules in the appeal cases of five leading businessmen operating in Russia against their sanctions imposed by the Council of the Europoean Union (C-696/23 (*Pumpyanskiy*), C-704/23 P (*Khudaverdyan*), C-711/23 P (*Rashnikov*), C-35/24 P (*Mazepin*) and C-111/24 P (*Khan*)). It upholds their freezing of funds, confirming that the criterion set out in Art. 2(1)(g) of Decision 2014/145/CFSP must be interpreted as meaning that the economic sectors concerned – not the individual businesspersons – must constitute a substantial source of revenue for the Russian government. Consequently, restrictive measures may be imposed on all influential businesspersons in such sectors, even if they themselves do not directly generate revenue for the state. The concept of „influence" within the meaning of the criterion is deemed to exist where a person plays a significant role in a sector of economic importance to the Russian government. Actual proximity to the government or the exercise of specific influence is not required. What is decisive is the economic significance of the person, assessed on the basis of factors such as position, activities, shareholdings and investments.

■ **30 March 2026:** The Commission adopts a €1.5 billion work programme under the European Defence Industry Programme to strengthen Europe's defence production and deepen cooperation with Ukraine. The programme includes €260 million for projects aimed at rebuilding and modernising Ukraine's defence industrial base, as well as further support for joint production, procurement, and defence innovation involving Ukrainian and EU industry.

■ **1 April 2026:** The EU receives €1.4 billion in proceeds from immobilised Russian Central Bank assets to support Ukraine. Most of the amount is channelled through the Ukraine Loan Cooperation Mechanism, while a smaller share supports Ukraine's military and defence needs through the European Peace Facility.

■ **1 April 2026:** The Commission takes steps to implement the €90 billion Ukraine Support Loan for 2026 and 2027. It proposes €45 billion in support for 2026, including budgetary assistance and funding for Ukraine's defence industrial capacities, and authorised procurement derogations to speed up drone purchases.

■ **15 April 2026:** The Commission announces €1.07 billion for 57 new European Defence Fund projects, including initiatives relevant to Ukraine's defence industry. The selected projects deepen cooperation with Ukrainian partners, include Ukrainian participation in drone-related cyber defence work, and allow Ukrainian entities to apply to sub-calls for start-ups and SMEs.

■ **21 April 2026:** The Council imposes sanctions on two entities over Russian hybrid activities, including propaganda and disinformation. The listings target Euromore, a pro-Kremlin media platform spreading narratives that justify Russia's war against Ukraine, and Pravfond, a Russian state-funded foundation used to reinforce disinformation claims about Ukraine and neighbouring states. The measures form part of the EU sanctions framework addressing Russia's destabilising activities against the EU, Ukraine, and other partners.

■ **23 April 2026:** The EU adopts its 20th package of sanctions against Russia, further tightening pressure on the Russian economy and its military-industrial base. The package includes new energy measures targeting Russia's shadow fleet, ports, and LNG-related services, as well as further restrictions on banks, crypto services, and payment channels used to circumvent sanctions. It also introduces additional trade restrictions, lists companies involved in military production and sanctions evasion, and activates the EU's anti-circumvention tool in response to re-exports of sanctioned goods to Russia for the first time. The package also includes new listings of individuals and entities, including actors linked to propaganda, the abduction of Ukrainian children, and the looting of cultural heritage.

■ **23 April 2026:** The Council finalises the legal framework for a €90 billion EU support loan to Ukraine, enabling the Commission to start disbursements in the second quarter of 2026. The loan is intended to cover Ukraine's urgent budgetary needs and to strengthen Ukrainian and European defence industrial capacities in 2026 and 2027. The Council also makes €45 billion available for 2026, including €16.7 billion in macro-financial and Ukraine Facility support and €28.3 billion for Ukraine's defence industrial capacities.

■ **30 April 2026:** The European Parliament adopts a resolution demanding accountability for Russia's attacks on civilians and civilian infrastructure in Ukraine. MEPs support the rapid establishment of the Special Tribunal for the Crime of Aggression against Ukraine and stress that responsibility should extend to those directing or enabling international crimes; the EP also reaffirms support for the ICC investigation, calls for stricter application and expansion of EU sanctions against Russia, and gives its consent to the International Claims Commission for Ukraine as a mechanism to support compensation for civilian victims.

■ **1 May 2026:** EU leaders reaffirm their support for Ukraine at an informal summit in Cyprus. President *Ursula von der Leyen* and European Council President *António Costa* meet with Ukrainian President *Volodymyr Zelenskyy* and welcome the adoption of the €90 billion Ukraine Support Loan and the 20th sanctions package against Russia.

■ **8 May 2026:** The Commission publishes the 2026 Eurobarometer, showing continued public support for EU action in response to Russia's war against Ukraine. According to the survey, most respondents see Russia's invasion as a threat to EU security and support continued assistance to Ukraine, including financial and humanitarian aid, sanctions against Russia, and aid until a just and lasting peace is reached.

■ **11 May 2026:** The Council expands the mandate of EUAM Ukraine to support Ukraine in countering hybrid threats and reintegrating veterans into civilian security and civil protection structures. The mission's new tasks include support for critical infrastructure protection, cyber-security, and countering foreign information manipulation, while continuing its work on civilian security sector reform and investigations of international crimes.

■ **11 May 2026:** The Council imposes sanctions on 16 individuals and seven entities linked to the unlawful deportation and forced transfer of Ukrainian children to Russia and occupied territories. The listings target actors involved in forced assimilation, indoctrination, militarised education, and unlawful adoption, including youth centres, military-patriotic organisations, and officials in Russian-occupied territories.

■ **11 May 2026:** The EU, Ukraine, Canada, and international partners hold a high-level meeting in Brussels on the return of Ukrainian children forcibly transferred or unlawfully deported by Russia. Participants agree to strengthen tracing, verification, and monitoring efforts, support Ukrainian authorities and civil society in securing returns, expand diplomatic engagement, and reinforce accountability for unlawful deportation, "re-education," and militarisation. The EU also announces an additional €50 million to support child protection and education.

■ **15 May 2026:** The Council of Ministers of the Council of Europe adopts a Resolution „establishing the Enlarged Partial Agreement on the Management Committee of the Special Tribunal for the Crime of Aggression against Ukraine". This is an important step towards the practical implementation of the Special Tribunal, which is tasked to investigate, prosecute and try individuals who bear the greatest responsibility for the crime of aggression against Ukraine; it was established by a bilateral treaty between the Council of European and Ukraine on 25 June 2025. The Enlarged Partial Agreement ensures the financing of the Special Tribunal as well as support for its operation by State Parties. The Agreement is supported by 34 Council of Europe Member States, the European Union, Australia, and Costa Rica. The EU supports the tasks of the Special Tribunal by the International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA) at Eurojust, which may pass investigations to the future tribunal. Funding of this Centre was ensured until December 2026. Furthermore, the EU financially supports the Tribunal by €10 million.

■ **19 May 2026:** The European Parliament approves revised rules on foreign investment screening in sensitive sectors such as defence, artificial intelligence, semiconductors, critical raw materials, and financial services. The reform makes screening mandatory for all Member States and seeks to protect EU security and public order in light of growing geopolitical risks, including Russia's war against Ukraine.

■ **21 May 2026:** In the preliminary ruling proceedings C-483/23 (*T Trust*), and Joined Cases C-428/24 (*FZ AR*) and C-476/24 (*SX*), the ECJ rules that the freezing of assets held by trusts is compatible with EU law where there is actual or economic attribution to sanctioned or designated persons. The three cases concern the freezing of funds and economic resources indirectly linked, via trust structures, to persons subject to EU restrictive measures in connection with Russia's military aggression against Ukraine. The ECJ finds that, in order to ensure the *effet utile* of EU law, the terms „belonging to" and „control" must be interpreted broadly. Applied to trust arrangements, this means that funds placed into a trust by a settlor listed on the sanctions list may continue to be regarded as his property or as being under his control, provided that he continues to exercise actual or legal influence over them or derives economic benefit from them. This applies mutatis mutandis to beneficiaries of a trust. This interpretation is in line with the concept of „freezing of funds and economic resources" in Regulation (EU) No. 269/2014, which aims to prevent, as much as possible, all possible uses of and transactions involving the assets in question. In addition, this aligns with the objective of restrictive measures, namely the protection of Ukraine's territorial integrity and maintenance of international peace and security, which require that any circumvention of those measures be prevented. Consequently, *de facto* influence and the ability to use such assets must also be taken into account.

■ **28 May 2026:** The Council approves the seventh regular payment under the Ukraine Facility, allowing Ukraine to receive nearly €2.8 billion. The payment follows Ukraine's completion of several reform steps under the Ukraine Plan, including measures related to public financial management, the judiciary, anti-corruption and anti-money laundering, financial markets, public assets, human capital, and the business environment. The Ukraine Facility provides over €50 billion in grants and loans for Ukraine's recovery, reconstruction, and modernisation from 2024 to 2027, with disbursements linked to reform progress and EU accession-related commitments.

■ **29 May 2026:** The Council appoints *Cornelia Taylor* as the new Head of Mission of EUAM Ukraine, with effect from 1 July 2026. EUAM Ukraine supports civilian security sector reform in line with EU standards and Ukraine's accession-related commitments. Since Russia's full-scale invasion, the mission has also assisted Ukrainian authorities with the investigation and prosecution of international crimes, integrated border management, and support in liberated territories. Its mandate was recently broadened to include countering hybrid threats and supporting veteran reintegration (see above).

■ **3 June 2026:** The European Parliament's Foreign Affairs Committee adopts a report on Ukraine's reform progress and EU accession path. MEPs welcome Ukraine's efforts to strengthen democratic institutions, judicial reform, and anti-corruption measures during the war, while calling for continued safeguards for the rule of law, media freedom, and independent anti-corruption bodies. They stress that Ukraine must be directly involved in any peace negotiations and reiterated that Russia should pay for the damage caused by its war of aggression.

■ **10 June 2026:** EP and Council negotiators reach a provisional agreement on measures to strengthen EU defence readiness and speed up defence investment. The deal simplifies permits, procurement, and intra-EU transfers of defence-related products, while also facilitating the implementation of the European Defence Fund. In relation to Ukraine, the agreement allows costs linked to testing in Ukraine to be eligible for EDF funding, thereby supporting closer cooperation with Ukrainian entities and the integration of battlefield experience into European defence projects.

■ **15 June 2026:** The EU and Ukraine open accession negotiations on the "fundamentals" cluster, marking the first negotiating cluster opened in

Ukraine's accession process. The cluster covers core areas such as the rule of law, fundamental rights, democratic institutions, public administration reform, and economic criteria. It includes the chapters on judiciary and fundamental rights, justice, freedom and security, public procurement, statistics, and financial control. Progress under this cluster will shape the overall pace of Ukraine's accession negotiations;

- **15 June 2026:** The Council adopts new sanctions targeting Russia's war economy, hybrid activities, and human rights violations. The package lists 34 individuals and 47 entities, including companies supporting Russia's military-industrial complex, suppliers of drones and military equipment, and actors involved in the shadow fleet used to export Russian oil. It also targets propagandists spreading narratives in support of Russia's war against Ukraine and renews the restrictive measures linked to Russia's illegal annexation of Crimea and Sevastopol until 23 June 2027. (AP/TW)

Course on AI, Justice, and the Rule of Law

UNESCO has launched a free online course on artificial intelligence and its use in judicial systems. The programme, entitled *AI, Justice, and the Rule of Law*, was developed together with the Saïd Business School, the Blavatnik School of Government, and the Faculty of Law at the University of Oxford, with support from the European Union.

The course examines how AI technologies are increasingly being integrated into judicial practice, including legal research, evidence analysis, real-time translation, case management, and risk or sentencing assessments. Against this background, the programme focuses on how courts and legal professionals could make use of AI while safeguarding human rights, judicial independence, procedural fairness, and public trust.

Particular attention is paid to questions of algorithmic bias, transparency, and accountability. The course addresses how judges should evaluate AI-generated outputs presented in court proceedings, what safeguards are needed to avoid overreliance on automated systems, and how judicial systems could introduce technological innovation without undermining the rule of law. Other modules focus on access to justice, fair trial rights, explainability of AI systems, and the impact of AI on women and marginalised groups.

The programme consists of approximately 18 hours of self-paced learning and includes expert-led video sessions, comparative case studies, practical exercises, and scenario-based discussions. It is aimed at legal professionals and judicial actors worldwide.

The academic direction of the course is provided by Professor *Ignacio Cofone* and Professor *Philippa Webb* of the University of Oxford. According to UNESCO, the programme draws on international human rights law, UNESCO's Global Toolkit on AI and the Rule of Law for the Judiciary, and comparative research on AI governance and judicial systems.

The course is initially offered in English, with French and Spanish versions expected to be available from June 2026 onwards. Participants who complete the programme receive a digital certificate issued by the Saïd Business School in cooperation with UNESCO and the University of Oxford partners. (AP)

Artificial Intelligence (AI)

EDPB and EDPS Warn against Weakening AI Act Safeguards

On 20 January 2026, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted Joint Opinion 1/2026 on the Commission's proposal for a Digital Omnibus on AI, which seeks to simplify the implementation of the AI Act. The proposal was tabled in 19 November 2025, including a wide range of measures to extend regulatory simplifications and reduce burdens.

The EDPB and EDPS support the general objective of addressing implementation challenges and reducing administrative burdens. However, they stress that simplification must not weaken the protection of fundamental rights, especially the rights to privacy and data protection.

A central concern is the proposed extension of the legal basis that allows providers and deployers to process special categories of personal data for bias detection and correction. While the EDPB and EDPS accept that such processing may be necessary in some cases, they warn that it must remain narrowly circumscribed. They recommend keeping the current standard of strict necessity, particularly to prevent broad or abusive reliance on this exception for non-high-risk AI systems.

They also oppose removing the obligation to register certain AI systems in the EU database when providers claim that systems listed in Annex III of the AI Act are not high-risk. In their view, this would weaken transparency and accountability and could incentivise providers to rely too easily on exemptions.

Regarding EU-level AI regulatory sandboxes, the EDPB and EDPS welcome their creation but call for clearer involvement of competent data protection authorities. They also recommend giving the EDPB an advisory role and observer status in the European Artificial Intelligence Board where data protection issues arise.

The Opinion further raises concerns about supervision by the AI Office,

stressing the need to clearly delimit its exclusive competence and to preserve the EDPS's role regarding AI systems used by EU institutions. It also warns against weakening the current AI literacy obligation for providers and deployers, arguing that AI literacy is essential for awareness of risks and compliance.

Lastly, the EDPB and EDPS express concern about delaying the application of high-risk AI rules. While acknowledging implementation challenges, they warn that postponement could affect fundamental rights protection in a rapidly evolving AI landscape and invite the co-legislators to consider maintaining the current timeline for certain obligations, such as transparency. (AP)

Digital Space Regulation

Two Years of the Digital Services Act

On 17 February 2026, two years after its applicability, the Commission took stock of the achievements of the Digital Services Act (DSA). Online platforms in the EU reversed nearly 50 million content moderation decisions following user appeals. This reflects a significant expansion of user rights, allowing individuals to challenge actions such as content removal, account suspension, or reduced visibility.

Overall, around 30% of the 165 million moderation decisions contested through internal platform mechanisms were overturned. Out-of-court dispute settlement bodies played an increasing role in resolving conflicts. In the same period, they reviewed more than 1,800 cases involving major platforms such as Facebook, Instagram, and TikTok, overturning platform decisions in 52% of resolved disputes. These mechanisms offer users a faster and more accessible alternative to judicial proceedings.

The regulation enhances transparency by granting researchers and civil society greater access to platform data and moderation practices, enabling closer scrutiny and accountability of digital services operating in the EU (→eucrim 2/2022, 228–230).

As part of its ongoing coverage of the DSA, *eucrim* has been tracking key developments and implementation trends, including a recent overview of regulatory and enforcement updates between November 2025 and February 2026 (→eucrim 4/2025). This reporting highlights the growing role of the DSA in shaping platform governance and content moderation practices across the EU. (AP)

Legislation

Illicit Trafficking of Firearms: New Legislative Proposal

spot light

On 26 February 2026, the European Commission presented a proposal for an EU Directive on combating firearms trafficking and other firearms-related offences (COM(2026) 102 final). The proposal pursues three different aims:

- Harmonising definitions and penalties for firearms-related criminal offences;
- Improving cross-border cooperation;
- Establishing a minimum dataset on firearms seizures.

Regarding the harmonisation of the EU Member States' criminal law, the Commission proposes that the EU Member States criminalise certain acts, provided that they are committed intentionally. These include:

- Trafficking and manufacturing of illicit firearms (maximum penalty of at least 8 years of imprisonment);
- Possession of illicit firearms, essential components and ammunition (maximum penalty of at least 5 years);
- Marking tampering, i.e, falsifying or illicitly removing or altering firearm markings (maximum penalties of at least 4 years);
- 3D printing of firearms, i.e., illicit creation, acquisition, possession and dissemination of blueprints (maximum penalty of at least 2 years).

The criminalisation of illicit manufacturing, illicit trafficking, and falsification and modification of markings on firearms will align EU law with the UN Firearms Protocol. The criminalisation of illicit possession derives from the Firearms Directive (EU) 2021/555. The offences relating to blueprints are intended to close a legal loophole and are considered new offences.

Alongside the definition of offences and „maximum minimum" penalties for natural persons, the proposal also includes provisions on the criminalisation of inciting, and aiding and abetting the commission of said criminal offences, liability and penatlies of/for legal persons, aggravating and mitigating circumstances, limitation periods, and jurisdiction.

To strengthen of cross-border cooperation, the Commission proposes an obligation for Member States to establish a National Firearms Focal Point. These Points should be tasked with the following:

- Gathering data on firearms and acting as a central hub for collecting available national data;
- Preparing a regular intelligence picture;
- Serving as a contact point for cooperation in international fora.

Improved data collection and standardisation of the available data on firearms is to be ensured by the Member States' obligation to collect statistical data (e.g. on number of criminal offenses registered, court cases dismissed, prosecutions and convictions, seized firearms) and the establishment of a minimum dataset to register seized firearms (to be shared with Europol's Firearms Hub). This improved data collection is, among other things, designed to help Member States identify trends (e.g. how decommissioned firearms from conflict zones enter the

Union). It will also support targeted efforts to seize firearms, prevent proliferation and improve situational awareness.

Background: The proposal will complement other EU rules on firearms with a „criminal law component". Existing rules mainly focus on the handling of firearms in the EU's internal market. They regulate the legal acquisition and possession of firearms. Examples include the Firearms Directive 2021/555, which defines minimum common rules on the acquisition and possession of firearms in the EU, as well as on the transfer of firearms from one EU country to another. The Firearms Regulation (recast in 2025) implements Art. 10 of the UN Firearms Protocol, laying down rules on the export of firearms. The UN Firearms Protocol, which the EU signed in 2014, also requires the criminalisation of illicit manufacturing and trafficking.

The presented proposal is the first legislative initiative to be adopted under the new European Internal Security Strategy, ProtectEU (→eucrim 1/2025, 3–4). The Strategy identified firearms trafficking as a major internal security threat to the EU, considering a criminal law response across the EU to be a major priority. (TW)

Institutions

European Parliament

New Parliament-Commission Framework Agreement

On 11 March 2026, the European Parliament (EP) approved a revised Framework Agreement between itself and the European Commission. The revision further develops an existing 2010 Agreement, reflecting over a decade of institutional practice and the evolving role of the EP during that time. The Parliament-Commission Framework Agreement establishes rules for cooperation in legislative, budgetary, and political matters. The revision was kicked off in October 2024, shortly after the EP elections. In September 2025, the EP and the Commission concluded the negotiations on the updated text.

Under the new agreement, the EP may, *inter alia*, call on the Commission to revise and withdraw existing legislation (negative right of initiative). In the case of urgent procedures and international agreements, stricter obligations regarding the provision of information and consultation with MEPs apply. Where the Commission proposes the provisional application of international agreements to the Council (prior to approval by the EP), it must, where possible, allow MEPs sufficient time to give their consent. Ultimately, the Agreement includes reinforced commitments to ensure a better presence of responsible Commissioners in plenary and committees, as well as the participation of the Commission in other parliamentary activities, when requested. (TW)

ECJ: Lifting of Immunity for Puigdemont and His Associates Null and Void

In its judgment of 5 February 2026, the ECJ set aside a judgment of the General Court and annulled three decisions by the European Parliament (EP) to waive the immunity of *Carles Puigdemont, Antoni Comín* and *Clara Ponsatí*. According to the ECJ, deciding upon appeal (Case C-572/23 P), the EP's decision must be considered invalid, because the appointment of the EP's rapporteur for the case was contrary to the requirement of impartiality.

➤ *Background to the case*

The case before the ECJ concerns three Catalan politicians who were elected to the EP in 2019 after criminal proceedings had been initiated against them in Spain on charges of alleged rebellion and embezzlement of public funds in connection with the 2017 independence referendum in Catalonia, for which the politicians were responsible. The Spanish judiciary had requested the EP to waive their immunity, which it did in 2021.

➤ *The ECJ's decision*

The ECJ has now ruled that the appointment of the rapporteur who reported on the requests to waive immunity breached the requirement of impartiality. While the EP had established rules to avoid close ties, it failed to consider that the rapporteur belonged to the same political group as members of a party that had instigated the criminal proceedings.

The ECJ clarified that the EP should also have prevented a rapporteur from acting who belonged to a political group with a factual connection to the criminal proceedings. Membership of the political group in question could give rise to doubts as to impartiality. The General Court in the previous instance (Case T-272/21) had not sufficiently taken this into account.

As the rapporteur was not impartial, the reports should have been regarded as null and void. Decisions based on these reports are therefore also null and void. Parliament must now start the whole process again from the beginning. (TW)

Court of Justice of the European Union (CJEU)

ECJ: Court of Last Instance Must Justify Refusal to Refer

On 24 March 2026, the ECJ ruled in the *Remling* case (C-767/23) that a national court of last instance must always provide reasons for refusing to refer questions to the Court of Justice of the EU for a preliminary ruling. Even if such a court or tribunal is permitted to dismiss appeals with a summary statement of reasons, it must in any case explain specifically and concretely why one of the exceptions to the ob-

ligation to refer questions for a preliminary ruling applies.

In its reasoning, the ECJ calls to mind the fundamental role of the preliminary ruling procedure in general and the obligation to refer in particular for the judicial system of the European Union. An exemption from the obligation to refer exists only in the three exceptional cases set forth in the CILFIT ruling: the lack of relevance to the decision of the question of EU law raised; the existence of a decision by the Court of Justice in which the relevant provision of EU law has already been interpreted; or the existence of an "acte clair." If courts decide against a referral, they must, taking into account the relevant factual and legal circumstances, set out concretely and specifically the reasons why one of these three exceptions would apply. A mere brief standard justification is not sufficient.

While the court of last instance may adopt the reasoning of a lower court, the lower court must, for its part, have explained why a question of EU law is not relevant to the decision, has already been clarified, or is unambiguous.

The background to the case was a legal dispute in the Netherlands in which a Moroccan family applied for a residence permit valid throughout the territory of the EU. Their appeal against the refusal of the permit was unsuccessful all the way up to the Dutch Council of State.

Overall, the ECJ's decision in *Remling* strengthens the preliminary ruling procedure under EU law (Art. 267 TFEU). In practice, this means that the pressure on supreme courts to provide reasoning is increased, which can result in a noticeable additional burden, particularly when dealing with a high caseload. (TW)

CJEU: Judicial Statistics 2025

On 20 March 2026, the Court of Justice of the European Union (CJEU) published its judicial statistics for the year 2025. In total, 1,878 new cases were brought before the Court of Justice (ECJ) and the General Court, while 1,898 cases were completed (including a series of 404 essentially identical joined cases as one case). There are currently 2,489 cases pending before both Courts. These figures confirm a continued high level of judicial activity, with a further increase in completed cases and a continued reduction in the overall number of pending cases compared with previous years (for the 2024 statistics →eucrim news of 29 April 2025).

The key figures for the ECJ:

- In 2025, the ECJ received 889 new cases, slightly fewer than in 2024 (920). However, without the transfer of certain preliminary ruling competences to the General Court, the number would have reached 954 cases, close to record levels.
- The ECJ completed 774 cases, reflecting sustained judicial activity comparable to previous years (excluding the exceptional year of 2024).
- As of 31 December 2025, 1,322 cases were pending before the ECJ, an increase compared to 1,207 in 2024, due to an imbalance between incoming and resolved cases.
- Requests for preliminary rulings continued to originate from almost all Member States, with particularly high numbers from Italian courts (110 requests) and Polish courts (63 requests).
- The average duration of proceedings decreased from 17.7 months in 2024 to 16.7 months in 2025. This reduction applied across all categories:
  - Preliminary rulings: from 17.2 to 16.9 months;
  - Direct actions: from 21.5 to 20 months;
  - Appeals: from 18.4 to 15.1 months.

The key figures for the General Court:

- In 2025, the General Court experienced a record level of activity. A total of 989 new cases were brought before it, marking a 26% increase compared to 2024 and the highest number in its history.
- The General Court closed 1,124 cases (or 1,527 when counting all related cases individually), an increase of 22% compared with 2024, representing the highest number of completed cases in a single year in the history of the General Court.
- Despite the influx of new cases, the backlog was reduced to 1,167 pending cases, the lowest level in 18 years.
- The average duration of proceedings decreased significantly. While the raw average was 18.9 months, the adjusted average duration was 16 months (down from 18.5 months in 2024).

In terms of subject matter:

- Litigation concerning restrictive measures (notably related to Russia's war against Ukraine) increased significantly, with 105 new cases.
- Civil service cases rose sharply (by 43%).
- Intellectual property cases decreased slightly.
- Cases relating to economic and monetary policy continued to decline.

Additionally, 2025 marked the first full year of the reform transferring certain preliminary ruling competences to the General Court. A total of 65 such cases were handled, mainly in areas such as VAT, transport passenger rights, customs law, and excise duties.

Overall, the statistics confirm that both courts continue to operate at a very high level of activity while improving efficiency, particularly through reduced procedural duration and structural reforms aimed at redistributing the workload between the ECJ and the General Court. (CR)

OLAF

The OLAF Report 2025

spot light

In 2025, OLAF recommended the recovery of €597 million of misused EU funds to the EU

budget and prevented €18 million from being unduly spent from the EU budget. The Office concluded 209 cases including recommendations for follow-up to the relevant national and EU authorities. In addition, 254 new investigations were opened after having analysed over 1140 reports on fraud and irregularities. These are the key figures of OLAF's annual report for the year 2025, which was presented on 20 April 2026. It is also available in digital format. For the 2024 report →eucrim 2/2025, 124.

For the first time, OLAF's annual activity report includes recommendations to stakeholders designed to foster a more effective and coordinated approach to combating fraud and irregularities. The report also provides a breakdown of how much OLAF recommended for recovery over the past 10 years. Accordingly, OLAF's recommendations led to the recovery of €5.9 billion and €873 million have been prevented from being unduly spent as a result of OLAF's investigations between 2016 and 2025.

With regard to the main trends in 2025, OLAF observed the following:

- Most investigations concerning expenditure fraud dealt with manipulation of procurement procedures, conflicts of interest, and inflated invoices. These trends also appeared in the 18 cases investigated linked to the Recovery and Resilience Facility (RRF);
- Revenue fraud investigation mostly concerned tobacco and e-cigarette smuggling, trade diversion, and evasion of customs duties and VAT. OLAF seized over 427 million illicit cigarettes worldwide, with 219 million cigarettes confiscated at the EU's external borders;
- OLAF conducted several high-profile investigations within the EU institutions. These increasingly involve cooperation with the EPPO. Cases included breaches of ethics rules, harassment, and abuse of teleworking rights.

With regard to anti-fraud policy developments, the report highlights the ongoing review of the European Anti-Fraud Architecture (AFA, →eucrim 2/2025, 137–138). This review process aims to improve coordination, efficiency and overall protection of the EU's budget against fraud and irregularities; for OLAF, strengthening cooperation with the EPPO, other EU law enforcement bodies, as well as national authorities and private partners remains key in this context. The report also points out that the AFA review goes hand in hand with the new multiannual financial framework (MFF) that envisages a fundamental overhaul of the EU financial approach and may lead to new challenges for preventing and combating fraud.

With regard to the perspectives of the future anti-fraud approach, OLAF formulates several recommendations, including the following:

- Invest in advanced technologies and data analytics to support investigations and improve the detection of fraud and irregularities;
- Establish a more coordinated and enhanced cooperation between OLAF and the other AFA partners, including secure and direct information exchange;
- Ensure OLAF has full access to the EU Customs Data Hub to facilitate the detection and prevention of customs fraud and other illicit activities;
- Support the strengthening of cooperation between OLAF and the Anti-Money Laundering Agency and the Member States' Financial Intelligence Units;
- Implement a coordinated EU approach to the regulation of e-cigarettes to reduce the difficulties faced by enforcement authorities in combating the illicit trade of e-cigarettes.

In its statement on occasion of the release of the OLAF report 2025, new OLAF Director-General, *Petr Klement*, emphasised that the Office must be staffed with adequate resources to carry out its mandate properly. Over the last 15 years, OLAF lost 110 permanent position and currently faces a concerning lack of human resources. (TW)

Successful Crackdown on Pharmaceutical Crime (Operation SHIELD VI)

On 25 February 2026, OLAF and Europol informed of the results of the joint law enforcement operation SHIELD VI. Now in its sixth year, this operation resulted in the prosecution of over 3,350 individuals, and the seizure of illicit medicines and doping substances worth over €33 million. Authorities from 30 countries, supported by OLAF, the EU Intellectual Property Office (EUIPO), Frontex, INTERPOL, and the World Anti-Doping Agency (WADA), carried out the joint operation between April and November 2025.

The operation focused on counterfeit and falsified medicines, the trafficking of anabolic-androgenic steroids and other doping substances, illegal food and sport supplements, and counterfeit sanitary products and medical devices. A total of 907 investigations were launched, 43 organised crime groups were investigated, and 66 websites were taken down.

Europol observed the following trends as a result of Operation SHIELD VI:

- An increased threat of poisoning and overdose due to abnormal medicine consumption outside a medical framework, such as the proliferation of counterfeit semaglutide-based products used as fat burners and the increasing availability of fake medicines containing potent synthetic substances.
- Criminals exploit the growing demand for medicines by these behaviours. Europe faces challenges due to the misuse of prescription and over-the-counter medicines for non-therapeutic purposes as well as the proliferation of online trafficking channels, particularly through unregulated websites.

■ Social media and online marketplaces, both on the surface web and on the dark web, continue to be central to the trade of counterfeit pharmaceuticals, as they provide anonymity and target large audiences.

■ Criminal networks typically operate one or more underground laboratories where they manufacture illicit pharmaceuticals and doping substances using raw ingredients.

Giving examples of operational success stories, Europol concluded that a multi-faceted approach is essential to effectively combat pharmaceutical crime. This approach should integrate health regulation, criminal justice cooperation, and public awareness campaigns.

OLAF Director-General, *Petr Klement*, emphasised the critical role of cross-border cooperation and interinstitutional cooperation with Europol in tackling counterfeit goods before they reach consumers: "The trade in illegal medicines represents a persistent and evolving threat, not only to public health but also to the integrity of the legal supply chain. By combining efforts, OLAF, Europol, and national customs authorities have safeguarded European consumers from dangerous health products". (TW)

OLAF Operational Work: First Half of 2026

This news item highlights key cases that demonstrate OLAF's operational work between 15 January and 30 June 2026. It follows on from the report in eucrim 4/2025, 266. The overview is in reverse chronological order.

■ **25 June 2026**: OLAF reports that it successfully supported the Italian and Turkish authorities in identifying tons of illegally shipped textile waste. These shipments, which were intended to circumvent strict and expensive EU recycling rules concerning textiles with non-biodegradable substances, were sent from Italy to Turkey. OLAF inspectors, alongside their Italian counterparts, also took part in on-the-spot inspections organised by the Turkish authorities. These inspections revealed additional textile waste stored in Turkish warehouses. For more information on OLAF's role in combatting illegal waste trafficking, see below.

■ **5 June 2026:** OLAF informs about its support of an operation targeting counterfeit truck parts. After having provided analyses and information, and coordinating with national authorities and brand owners in several EU countries, the operation led to the seizure of 14,629 counterfeit items worth more than €600,000 in Portugal. The parts had been manufactured in Türkiye and illegally imported into the EU. They pose serious risks to road safety.

■ **26 May 2026**: OLAF and Eurojust report on the successful conclusion of the operation „Coals of the Alps" that dismantled a criminal network involved in illegal waste trading. Since 2022, Italian authorities have been investigating several companies and officials who established an illegal scheme that transformed ash containing highly toxic materials into supposedly environmentally friendly charcoal for use in barbecue briquettes, fertilisers and concrete additives. This not only circumvented bans but also harmed consumers and the environment. OLAF provided analyses of the scale of the illegal traffic and supported information-sharing. Eurojust coordinated the execution of European Investigation Orders and European Arrest Warrants.

■ **6 May 2026**: A joint operation between Polish and Spanish customs reveals an illegal textile diversion scheme. OLAF supported and coordinated this operation. The Office analysed trade flows and found that consignments of textile products from China had been falsely declared as being in transit despite not having left the EU. This scheme circumvented high customs duties payable on textile products entering the EU. Following controls initiated by OLAF, the Polish customs authorities seized three containers loaded with almost 70,000 kilograms of textiles.

■ **28 April 2026**: Thanks to OLAF's support, a complex VAT and customs fraud scheme is dismantled. Through false confirmations and misdeclarations, a criminal network simulated intra-Community movements of goods that were imported from China via the Polish-Belarusian border. In reality, the goods (textiles, footwear, electric bicycles, etc.) were removed from transit and remained in Poland. This resulted in the evasion of approximately €118 million in customs duties and €79 million in VAT, representing a significant loss to the EU budget. The operation involved several EU Member States, including Belgium, Slovenia, Germany, Hungary and Poland. The EPPO in Poland continued a criminal investigation into the criminal network, while OLAF further conducts complementary investigations.

■ **17 April 2026**: OLAF announces the results of Joint Customs Operation (JCO) VAPE, which resulted in the seizure of over 94 million pieces and over 2,500 kg/l of tobacco products, e-cigarettes, and devices. This was the first international JCO to focus on the illicit trade in e-cigarettes and heated tobacco products. The JCO was carried out between 14 November to 15 December 2025, involving 23 EU Member States and seven partner countries outside the EU. OLAF stresses that the findings of JCO VAPE would contribute to mapping new trafficking patterns, identifying key routes and modus operandi, and strengthening the basis for future enforcement actions and risk analysis.

■ **13 February 2026:** Albanian authorities uncover and stop illegal shipments of hazardous waste from Albania to Thailand following support by OLAF. As early as 2024, OLAF had alerted Albanian customs authorities

to a shipment suspected of containing large quantities of misdeclared hazardous waste. It was found that companies had declared a toxic by-product of steel production as non-hazardous „iron oxide", which can be legitimately used in the EU for several industrial applications. OLAF is becoming increasingly involved in the fight against illegal waste trafficking. OLAF's support in Member State investigations into waste trafficking is reinforced by the Waste Shipment Regulation (→*L. I. Garruto* and *S. Grassin*, „Fighting Waste Trafficking in the EU: A Stronger Role for the European Anti-Fraud Office", eucrim 2/2024, 143–145). Due to the complex and transnational nature of illegal waste shipments, OLAF's involvement helps ensure that customs, environmental and judicial authorities can act swiftly and in a coordinated manner to prevent environmental damage and protect public health.

■ **28 January 2026:** An international investigation, coordinated and supported by OLAF, reveals a large-scale criminal scheme that was circumventing restrictive measures against Russia in relation to the export of vehicles. Through extensive data analysis and cross-checking of customs, trade, and transport information and by tracking vehicles and reconstructing the logistics chain, OLAF discovered that more than 760 used vehicles from various EU Member States had been declared as destined for third countries such as Türkiye, whein in fact their final destination was Russia. OLAF's findings led to criminal investigations in three EU Member States. In addition, information shared by OLAF prompted the relevant EU authorities to strengthen the monitoring and risk profiling of future shipments. Acting Director-General of OLAF, *Salla Saastamoinen,* stated: "This investigation demonstrates how cooperation with Member States and third-country authorities enables OLAF to protect the integrity of EU sanctions." (TW)

European Public Prosecutor's Office (EPPO)

Hungary Joins EPPO – EPPO Regulation Now EU Acquis

spot light

On 10 July 2026, the Commission adopted a decision confirming Hungary's participation in the European Public Prosecutor's Office (EPPO). The decision was published in the Official Journal L, 2026/1701 of 13 July 2026. The request to join the EPPO was submitted by the new Hungarian government under Prime Minister *Péter Magyar* in May 2026. This is a historic step as the new government reverses the steadfast refusal to join the independent EU anti-fraud body by the previous Orbán administration.

Hungary must now appoint three candidates for the post of European Prosecutor at the central office in Luxembourg. The Council will nominate one of them. Hungary will also need to propose candidates for the posts of European Delegated Prosecutors to the European Chief Prosecutor.

Hungary is the 25th EU Member State who joined the enhanced cooperation scheme of the EPPO. Now, only Ireland and Denmark are not participating on the basis of opt-out reservations for justice and home affairs matters included in primary EU law. Therefore, Hungary's participation in the EPPO is also historic in other respects: With the entry into force of the aforementioned Commission Decision (on 2 August 2026), the EPPO Regulation 2017/1939 ceases to be an act adopted within the framework of enhanced cooperation and will become an ordinary act of Union law, and thus part of the *acquis*. This means that any new member state joining the European Union in the future will be required to join the EPPO.

President of the European Commission, *Ursula von der Leyen*, commented on 10 July 2026: „Today brings good news for Hungary. This is a welcome step in the fight against fraud and corruption. The people of Hungary will now have a safeguard in place to ensure EU funds work in their interest. Hungary, welcome to the European Public Prosecutor's Office." Commission Vice-President *Henna Virkkunen* and Commissioner for Justice, *Michael McGrath*, also highlighted the historic day for Hungary and the EU. (TW)

General Court Rules on EPPO Investigative Powers Vis-à-Vis European Court of Auditors

spot light

On 10 June 2026, the General Court of the EU delivered its judgment in Case T-99/25, *European Public Prosecutor's Office (EPPO) v European Court of Auditors*. The case concerned the question whether EU institutions may rely on unresolved immunity issues and confidentiality rules to prevent the EPPO from gathering evidence in the context of a criminal investigation and clarified the limits of institutional objections to EPPO investigative measures.

➤ *The cause of the legal dispute*

The case arose in the context of an EPPO investigation into alleged irregularities concerning the recruitment and appointment of an official of the European Court of Auditors (ECA). Following information transmitted by OLAF, the EPPO concluded that there was evidence of conduct potentially constituting an offence within its competence and formally opened a criminal investigation. As the ECA's premises, buildings, and archives benefit from the privileges and immunities of the EU and its officials enjoy immunity under EU law, the European Delegated Prosecutor handling the case requested that the European Chief Prosecutor seek to lift those protections. Several requests were subsequently submitted to the President of the ECA to lift the inviolability of the institution's premises, buildings, and archives, as well as

the immunity of the individuals under investigation. The President of the ECA declined those requests, on the basis that the information provided by the EPPO was insufficient to justify such measures. He also believed that those affected should be informed and given the opportunity to submit observations before any decision affecting their immunity was made. The ECA proposed meetings with EPPO representatives and provided documents relating to the investigation.

Subsequently, the European Delegated Prosecutor requested additional documents and sought to lift the duty of confidentiality applicable to 12 EU officials so that they could be heard as witnesses. While providing some of the requested documentation, the ECA reiterated its proposal for a meeting and ultimately rejected the request to lift the 12 officials' duty of confidentiality. In its statement of position, issued by the Head of Legal Service, the ECA concluded that the EPPO had failed to provide sufficient information concerning the suspected offences. It therefore concluded that lifting the 12 officials' duty of confidentiality would be contrary to the interests of the EU. It further argued that granting the request would effectively circumvent its earlier decision not to lift the immunity of the two individuals under investigation and stated that the investigation should therefore be discontinued.

The EPPO subsequently brought an action before the General Court of the EU, seeking the annulment of this statement of position, while the ECA contended that the action should be dismissed as inadmissible or, alternatively, as unfounded.

➤ *The ECA's arguments*

The ECA submitted that the contested statement of position does not constitute an act challengeable under Art. 263 TFEU. It argued that it could not lift the duty of confidentiality of the 12 officials, as it had not been provided with sufficient information to ensure that the requested measures would not harm the interests of the EU. Furthermore, the ECA claimed that the EPPO had based its request to lift the duty of confidentiality on Art. 19 of the Staff Regulations, which concerns employment relations between EU institutions and their officials, rather than on the prerogatives of investigative bodies and national judicial authorities. However, only a decision adopted by the competent appointing authority in the context of such an employment relationship would produce legal effects that could be reviewed by the CJEU. According to the ECA, this was not the case in the present matter.

Regarding the plea of inadmissibility, the ECA argued that, where immunity constitutes an obstacle to an investigation, requesting the lifting of the immunity of the persons under investigation is a necessary preliminary step. In its view, immunity is not a minor procedural issue but a legal obstacle that must be removed before an investigation can proceed effectively. Therefore, evidence obtained while immunity remains in place may not be admissible in proceedings against the protected persons. As the EPPO had not brought an action at the time to annul the President of the ECA's decisions refusing to lift the immunity of the two individuals concerned, it could not, at a later stage, seek to advance the investigation indirectly by requesting that officials be released from their duty of confidentiality.

➤ *The EPPO's arguments*

The EPPO countered that, in line with Art. 263(1) TFEU, the CJEU is responsible for reviewing the legality of acts issued by the institutions, bodies, offices, and agencies of the EU that are "intended to produce legal effects vis-à-vis third parties". This applies to all measures or provisions adopted by these bodies, whatever their nature or form, if they are intended to have binding legal effects. In the present case, the contested statement of position was sent in response to the request to lift the duty of confidentiality of 12 officials. It originated from the College of Members of the ECA, i.e., the competent appointing authority.

In consequence, the European Delegated Prosecutor could not hear the officials as witnesses, meaning that the statement produced legal effects vis-à-vis the EPPO. Any other interpretation allowing a decision by an EU institution, agency, body, or office refusing to lift an official's duty of confidentiality on the basis of Art. 19 of the Staff Regulations to have legal effects only in relation to the official concerned in proceedings under Art. 270 TFEU would prevent European Delegated Prosecutors from exercising their powers under Art. 28 of the EPPO Regulation. This would hinder the conduct of the investigation, as the EPPO would not be able to challenge the lawfulness of such a refusal before the CJEU.

Regarding the pleas of inadmissibility, the EPPO observed that no decision had ever been adopted by the competent body of the ECA refusing to lift the immunity of the persons under investigation. The letters sent by the President of the ECA could not be regarded as such decisions, since the President did not have the power to adopt them and the letters did not express the institution's final position. Consequently, as no final decision had been adopted, the EPPO could not be criticised for failing to challenge a refusal decision or for allowing the time limit for bringing an action against such a decision to expire.

➤ *The General Court's ruling*

The General Court (GC) first rejected the two pleas of inadmissibility raised by the ECA. The contested statement of position is a challengeable act that may the subject of an action for annulment under Art. 263 TFEU. In addition, since the ECA has not yet adopted a final decision in due and proper form

on the request to lift immunity, the EPPO retains a legal interest in bringing proceedings against the contested statement of position in so far as that position prevents it from gathering additional evidence that may enable it to substantiate the request to lift immunity or to find that there is no longer any need to continue the proceedings brought against the persons under investigation.

With regard to the substance, the GC held that the ECA had wrongly linked the request to lift the duty of confidentiality of the 12 officials to the request to lift the immunity of the persons under investigation. The request concerning the 12 officials related only to potential witnesses and had to be assessed independently under Art. 19 of the Staff Regulations. The ECA could therefore not refuse to release the officials from their duty of confidentiality merely because it had not granted the request to lift the immunity of the persons under investigation.

Second, the ECA had misconstrued the concept of the „interests of the Union" in the second sentence of the first paragraph of Art. 19 of the Staff Regulations. According to settled case law, that concept must be interpreted restrictively and covers only interests of considerable importance that are vital to the European Union.

The General Court found that the immunity of the persons under investigation could not, in itself, be regarded as such a vital Union interest justifying refusal to allow the 12 officials to testify. On the contrary, allowing the EPPO to gather evidence during an investigation, including through testimony from EU officials, serves the interests of the Union and enables the EPPO to exercise the investigative powers conferred on it by the EPPO Regulation.

In conclusion, the GC therefore upholds the action brought by the EPPO and annulled the contested statement of position. (CR)

2nd Edition of EPPO Commentary Published

The second edition of the Article-by-Article commentary on the EPPO Regulation has been published. The commentary was founded and is edited by Dr. Hans-Holger Herrnfeld, Prof. Dr. Dominik Brodowski, LL.M. (UPenn), and Prof. Dr. Christoph Burchard, LL.M. (NYU). It is published by the renowned *Nomos Verlag*. This commentary has become the leading English-language reference work on the legal framework of the European Public Prosecutor's Office (EPPO)

Since beginning operations in June 2021, the European Public Prosecutor's Office (EPPO) has established itself as the central authority for prosecuting offenses detrimental to the financial interests of the EU. The second edition of the commentary reflects all current developments and landmark judgments of the Court of Justice of the European Union, including:

- The EPPO's Rules of Procedure;
- Relevant CJEU case law concerning the EPPO, in particular
  - judgment C-281/22 on cross-border investigative measures, and
  - judgment C-292/23 on legal protection against investigative measures;
- Further decisions of the EPPO College on internal procedural rules and guidelines.

The volume also outlines considerations for extending the EPPO's mandate and for improving its legal framework in future. The second edition features an interesting new addition: practice-oriented country reports on the Member States participating in the establishment of the EPPO. These contributions provide a thorough and practice-focused analysis of how the EPPO is integrated into national criminal justice systems. The commentary addresses criminal law practitioners – including prosecutors, law enforcement authorities, courts, and law firms – and also serves as a reliable resource for academic research on the EPPO. (TW)

CJEU Confirms National Courts' Role in Reviewing EPPO Measures

On 16 April 2026, the Court of Justice (ECJ) delivered its appeal judgment in Case C-328/24 P, *Mincu Pătrașcu Brâncuși v EPPO*, concerning a challenge brought by a Romanian national against procedural actions taken by the European Public Prosecutor's Office (EPPO).

In an investigation opened by the EPPO in 2021 against *Mincu Pătrașcu Brâncuși*, the permanent chamber of the EPPO ordered that he be brought to trial before the competent Romanian criminal court in proceedings relating to alleged participation in a criminal organisation and fraud affecting the financial interests of the EU. The applicant sought to have this decision annulled before the General Court of the European Union (GC), arguing that it infringed his fundamental rights and should be subject to direct review at EU level. However, the GC dismissed the action as inadmissible for lack of jurisdiction (Case T-385/23). The matter was subsequently appealed before the ECJ.

In its judgment, the ECJ upheld the GC's conclusion and dismissed the appeal in its entirety. The Court held that, under EU law, jurisdiction to review procedural acts of the EPPO with legal effects vis-à-vis third parties lies, as a rule, with the national courts rather than the courts of the EU. The ECJ emphasised that EPPO investigations are closely integrated into national criminal proceedings and that the final determination of criminal liability rests with the competent national courts. Accordingly, challenges to EPPO procedural measures must ordinarily be

brought before national courts, which retain the ability to refer questions of EU law to the Court in Luxembourg under the preliminary ruling procedure where necessary.

At the same time, the ECJ confirmed that the EU legislature was entitled to establish such a system of judicial review in light of the institutional design and mandate of the EPPO, and that this framework does not infringe the right to an effective judicial remedy or to a fair trial. (CR)

Anti-Money Laundering Authority (AMLA)

AMLA Takes Over AML/CFT Powers from the EBA

On 31 December 2025, the European Banking Authority's (EBA) anti-money laundering and countering the financing of terrorism (AML/CFT) powers in the financial sector were formally transferred to the Anti-Money Laundering Authority (AMLA). This marks a key milestone in the EU's fight against financial crime. The handover concludes the EBA's standalone role in this area, which began in 2020, and places AMLA at the centre of a coordinated EU system for supervising anti-money laundering and counter-terrorist financing.

The two authorities worked together closely to ensure a smooth transition. Key EBA tools and expertise, including databases, supervisory insights, and risk assessments, have been transferred to AMLA. Existing EBA guidelines and standards will remain in effect until AMLA issues its own, ensuring continuity for both financial institutions and national supervisors.

Under the new framework, AMLA will complete the EU's Single Rulebook on Anti-Money Laundering, promote consistent supervision across Member States, and coordinate the work of Financial Intelligence Units (FIUs) to improve cross-border information sharing. AMLA will also directly supervise 40 of the EU's most complex financial institutions and groups. The EBA will continue to address money laundering risks through its banking oversight, working closely with AMLA to maintain a coherent system.

To support ongoing collaboration, the two authorities have established a formal Memorandum of Understanding in 2025, enabling regular information exchange, joint initiatives, and consistent engagement with the private sector. (CR)

AMLA Publishes First Single Programming Document for 2026–2028

On 4 February 2026, the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) published its first Single Programming Document (SPD) for 2026–2028, setting out its work programme and strategic priorities as it builds towards full operational capacity.

The SPD outlines AMLA's objectives across three core deliverables: (1) completion of the Single Rulebook, (2) advancement of supervisory convergence, and (3) strengthened cooperation among Financial Intelligence Units (FIUs).

These are implemented through five key workstreams:

- First, AMLA will focus on delivering its regulatory mandates, with 24 of 40 mandates scheduled for 2026. Central to this is the EU AML/CFT Single Rulebook, which aims to harmonise anti-money laundering rules across the EU, close regulatory gaps, and reduce fragmentation between Member States. AMLA will prioritise mandates that are critical for industry and essential to implementing its supervisory functions and supporting FIUs, ensuring that regulatory measures are both effective and practical.
- Second, AMLA will lay the groundwork for its direct supervision of high-impact financial institutions, set to begin in 2028. In 2026, the Authority will finalise the risk analysis and selection methodology, initiate data collection for testing and calibration, and define procedures for transferring supervisory information from national authorities to support the supervisory model.
- Third, AMLA will strengthen cooperation among EU FIUs, focusing on joint analyses, harmonised technical standards, and mediation mechanisms. Initial peer reviews will begin in 2026, and the optimisation of FIU.net will continue through 2027 to enable secure EU-wide information exchange.
- Fourth, to promote supervisory convergence, AMLA will develop common frameworks for indirect supervision across the financial sector and oversight in selected non-financial sectors. This includes harmonised supervisory models, manuals, and thematic reviews to guide national authorities and ensure consistent application of EU instruments.
- Fifth, AMLA will establish a robust risk analysis framework, mapping data sources and creating infrastructure to collect and analyse information. This will support the identification, assessment, and mitigation of money laundering and terrorist financing risks, forming the analytical backbone of its operations.

In addition to delivering its core tasks, AMLA will continue to scale up its operational capacity by recruiting new staff, investing in IT infrastructure to establish a secure and agile system, and consolidating internal governance structures. Over the coming years, the Authority will implement key regulatory mandates, develop and refine its risk frameworks, and gradually expand its supervisory and operational functions across the EU. It will also finalise the assessment methodology and prepare for the 2027 selection of entities for direct supervision. Throughout this process, AMLA will engage closely with national compe-

tent authorities and stakeholders to ensure that the new EU AML/CFT framework is robust, consistent, and fit for purpose. (CR)

AMLA Executive Board Now Fully Operational with Fifth Member Appointed

On 23 February 2026, the Council of the EU appointed *Hennie Verbeek-Kusters* as the fifth full-time member of the Executive Board of the Anti-Money Laundering Authority (AMLA), completing the governing body. The Executive Board is composed of the Chair and five full-time members, including the Vice-Chair, each appointed for a four-year term following a proposal from AMLA's General Board and approval by the European Parliament.

The appointment process began in January 2025, when the European Commission prepared a shortlist of candidates for the Executive Board and submitted it to the European Parliament. In March 2025, AMLA's General Board proposed five members – *Simonas Krėpšta*, *Rikke-Louise Petersen*, *Marcus Pleyer*, *Derville Rowland*, and *Juan Manuel Vega Serrano* – which the European Parliament approved in April 2025. Following the withdrawal of Mr *Pleyer* in May 2025, the Council appointed four members. Ms *Verbeek-Kusters* now joins the Board as the fifth full-time member.

Ms *Verbeek-Kusters* brings extensive expertise in financial intelligence to the table. She has led the Netherlands' Financial Intelligence Unit since 2008 and has twice served as Chair of the Egmont Group of Financial Intelligence Units, playing a key role in international cooperation against money laundering and terrorist financing.

With her appointment, AMLA's Executive Board is now fully operational and ready to steer the Authority as it implements its supervisory, regulatory, and operational mandates across the EU. (CR)

AMLA Holds First Public Hearing to Advance the EU AML Single Rulebook

On 24 March 2026, the Anti-Money Laundering Authority (AMLA) held its first public hearing to further develop the EU Anti-Money Laundering Single Rulebook into a robust, risk-based, and practical framework for all entities in the EU. The hearing provided stakeholders with an opportunity to speak directly with AMLA staff drawing up the draft standards, to ask questions, share experiences, and highlight areas requiring further clarification.

The first hearing brought together over 1,600 stakeholders, including obliged entities from the financial and non-financial sectors, as well as civil society organisations. The hearing was structured around two sessions, each dedicated to a draft standard that forms a cornerstone of the Single Rulebook.

The first session focused on the criteria for identifying business relationships, occasional transactions, and linked transactions. It explained how these distinctions determine when obliged entities must carry out customer checks, and how attempts to circumvent these checks by splitting transactions can be prevented.

The second session addressed customer due diligence, outlining the information and documentation that obliged entities should collect for standard, simplified, and enhanced due diligence procedures.

The slides on customer due diligence and business relationships presented during both sessions are available to download.

The public hearing is part of a wider consultation process. Written submissions on both Regulatory Technical Standards (RTS) were open until 8 May 2026. Input received during the public hearing will complement the written submissions and play a vital role in shaping the final standards.

Obligations for private entities to prevent the use of the financial system from money laundering and terrorist financing are now prescribed in the directly applicable Regulation (EU) 2024/1624, „the AML Single Rulebook" (→eucrim 2/2024, 117–118). It replaces the system to date that has regulated said obligations in five AML/CFT Directives. (CR)

AMLA's Inaugural Conference: EU Pushes for Stronger AML/CFT Coordination

On 9 June 2026, the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) held its first public conference, bringing together over 360 participants from all 27 EU Member States, with additional stakeholders following online via livestream. Attendees included representatives of EU institutions, national supervisory and law enforcement authorities, financial intelligence units, the private financial sector, technology firms, academia, and international organisations, covering the full spectrum of Europe's anti-money laundering ecosystem.

The conference took place to mark AMLA's first public engagement since its establishment and to signal its operational launch. According to the authority, the event aimed to assemble stakeholders across the EU to discuss evolving financial crime risks, foster cooperation, and support the implementation of anti-money laundering and counter-terrorist financing (AML/CFT) rules.

Convening at the Alte Oper in Frankfurt am Main, discussions centred on three main priorities:

- Improving the effectiveness of financial intelligence in detecting and investigating illicit activity;
- Strengthening consistency in supervision across EU Member States;
- Addressing emerging risks linked to artificial intelligence, crypto-assets, and digital financial services.

In her opening address, AMLA Chair *Bruna Szego* underlined that the fight

against money laundering is closely linked to the integrity of the EU's economy and financial system, and to Europe's broader autonomy, resilience and competitiveness. (CR)

Europol

Europol and Interpol Agree on Key Joint Operational Priorities

The cooperation between Europol and INTERPOL is based on an existing arrangement, signed in 2001, which provides the framework for the two organisations to agree on joint operational priorities and strengthen their cooperation in areas of common interest. Within this framework, Europol and INTERPOL agreed, at the end of May 2026, on a new set of Joint Key Operational Priorities (JKOP) to guide their cooperation against cross-border crime over the coming year.

Developed by operational experts from both organisations, the priorities aim to enhance coordination and support joint efforts when criminal networks operate across national borders. They cover key areas, including organised crime, cybercrime, economic and financial crime, and counter-terrorism, enabling a more coordinated and proactive response to evolving criminal threats. (CR)

Europol Launches European Centre Against Migrant Smuggling

On 24 March 2026, Europol launched the European Centre Against Migrant Smuggling (ECAMS) as part of the implementation of the new Pact on Migration and Asylum. The centre is intended to consolidate and strengthen existing Europol capabilities, leading to a more integrated, operationally focused structure against migrant smuggling. It is designed to reinforce Europol's support to EU Member States through four main principles: (1) data-driven analysis, (2) close operational proximity to ongoing investigations, (3) strengthened international cooperation, and (4) the disruption of criminal networks.

ECAMS provides operational, technical, and forensic support to Member States, with a focus on dismantling high-risk migrant smuggling networks. It offers capabilities in data-driven investigative support, open-source intelligence (OSINT), operational analysis, and strategic coordination, including stakeholder management and deployment capacity.

The centre is structured into two main units: the Migrant Smuggling Unit and the Expertise and Stakeholder Management Unit. The Migrant Smuggling Unit focuses on different trafficking routes, including land, sea, intra-EU secondary movements, and outbound flows. The Expertise and Stakeholder Management Unit brings together teams responsible for large-scale data analysis and online monitoring, operational deployment support at EU hotspots, and coordination with national and international stakeholders.

ECAMS builds on Europol's long-standing work in the field of migrant smuggling. Since the creation of the European Migrant Smuggling Centre (EMSC) in 2016 (→eucrim 1/2016, 7) Europol has gradually expanded its operational and analytical capacity, including the establishment of specialised teams for maritime operations, joint liaison structures, and operational task forces targeting smuggling and trafficking networks across multiple regions.

ECAMS represents the latest stage in this development, consolidating existing capabilities into a more structured and operationally integrated centre, with strengthened emphasis on integrated operational support, digital investigative capacity, and deployment-based assistance to Member States in combating migrant smuggling across physical and digital environments. (CR)

Search for New Executive Director of Europol

On 17 February 2026, Europol published a vacancy notice for the position of Executive Director. The current Executive Director, *Catherine De Bolle* (→eucrim 2/2022, 100), has held the office since 1 May 2018, with her mandate due to end on 1 May 2026.

The Executive Director is responsible for the day-to-day management of the agency, its strategic development, and the implementation of its mandate in accordance with the Europol Regulation. The position is subject to the supervision of the Management Board and requires accountability to the Management Board, the European Parliament, and the Council.

The recruitment procedure is governed by the Europol Regulation, the Staff Regulations of Officials of the European Union, the Conditions of Employment of Other Servants of the European Union, and the Management Board rules.

The Europol Management Board will establish a selection committee to review applications and conduct interviews. Candidates must be nationals of a Member State of the European Union, hold a university degree, and demonstrate at least 20 years of postgraduate professional experience, including a minimum of five years in a senior executive management function.

The process to appoint a new Executive Director is underway. Applications closed on 31 March 2026, and a selection committee set up by Europol's Management Board will conduct interviews and an assessment centre before the Board will submit a shortlist of at least three candidates. Under the Europol Regulation, the European Parliament will be consulted, while the final appointment decision will be made by the Council. The selection procedure is expected to continue for several months, with the appointment of a new Executive Director an-

ticipated by the end of 2026. The successful candidate will be appointed for a four-year term, renewable once.

On 2 May 2026, Europol entered a transition phase following the departure of Executive Director *Catherine De Bolle*, who stepped down on 1 May 2026 after eight years in office.

Following a decision of the Europol Management Board, *Jürgen Ebner* has assumed the role of Acting Executive Director during the transition period. Before joining Europol, where he has been working since November 2019, *Jürgen Ebner* held a senior position at the German Federal Criminal Police Office (*Bundeskriminalamt*). (CR)

Eurojust

JIT Points to Suspected Russian Intelligence Role in Parcel Fires

A Joint Investigation Team (JIT), set up and funded by Eurojust and supported by Europol, has exposed an operation involving self-igniting parcels. The team comprises authorities from Germany, Lithuania, Poland, the Netherlands, and the United Kingdom.

The JIT deals with several incidents that were recorded along transit routes of parcels that were sent from Lithuania to addresses in the UK and Poland in 2024. One parcel, which passed through a sorting centre in Germany, caught fire at Leipzig airport shortly before being loaded onto an aircraft. Another ignited in a warehouse in the United Kingdom, while a third caught fire in a truck in Poland.

Authorities were able to intercept one parcel before ignition, allowing for analysis of the device and its potential damage. The investigation also identified two "test packages" sent to the United States and Canada, as well as two parcels in Amsterdam intended for the same destinations.

Eurojust reported on 6 March 2025 that, according to investigators, suspected perpetrators were recruited and instructed via an online messaging service. Tasks were divided among several individuals, and payments were often made in cryptocurrencies. Investigators suspect the acts were carried out on behalf of the military intelligence service of the Russian Federation.

Eurojust continues to identify links to other investigations involving similar incidents, and to coordinate cooperation between the countries involved. (CR)

Eurojust and Genocide Prosecution Network Commemorate 2026 EU Day Against Impunity

On 23 May 2026, Eurojust marked the 11th EU Day Against Impunity for genocide, crimes against humanity, and war crimes – together with the Genocide Prosecution Network. Since 2016, Eurojust and the Genocide Prosecution Network have jointly highlighted the EU Day Against Impunity to raise awareness of core international crimes and strengthen cooperation between national authorities.

The commemoration took place against the backdrop of growing armed conflicts worldwide and increasing pressure on the international criminal justice system. Eurojust and its partners reiterated their shared commitment to ensuring accountability for the most serious international crimes and to supporting victims and survivors. Attention was drawn to the continued efforts of EU Member States in exercising extra-territorial and universal jurisdiction.

In 2025 alone, over 30 new cases were opened across more than 20 countries, reflecting sustained investigative and prosecutorial activity in relation to crimes committed in more than 30 states.

Recent judicial developments were also highlighted, including landmark convictions in Sweden for genocide through the transfer of children; the first convictions in the Netherlands and France for crimes committed against the Ezidi community; and ongoing proceedings in cases involving Rwanda and the Democratic Republic of the Congo. In Belgium, an indictment was filed in a case involving alleged war crimes and crimes against humanity committed in Liberia.

Progress in accountability for crimes committed in Ukraine was also underlined, including the work of the JIT on alleged core international crimes in Ukraine (→eucrim 1/2025, 8). In this context, a landmark conviction in Finland was highlihted, where a Russian national was found guilty on the basis of universal jurisdiction for war crimes committed in 2014.

Finally, Eurojust also underlined increasing efforts in the area of corporate accountability (legal responsibility of companies for participation in criminal conduct), with ongoing investigations into alleged corporate involvement in core international crimes. (CR)

Eurojust Vice-President Re-Elected

On 26 May 2026, Lithuania's National Member at Eurojust, *Margarita Šniutytė-Daugėlienė,* was re-elected as Vice-President of the Agency. She will begin her second four-year mandate on 28 June, continuing to serve alongside Eurojust President *Michael Schmid* and Vice-President *José de la Mata*.

Ms *Šniutytė-Daugėlienė* has served as National Member for Lithuania since 2019. Before joining Eurojust, she worked at the Regional Prosecutor's Office of Klaipėda, later becoming Chief Public Prosecutor of its 2nd Criminal Prosecution Division. She was appointed Deputy Prosecutor General of Lithuania in 2016, a position she held before joining the Agency.

During her first mandate as Vice-President, which began in June 2022, Ms *Šniutytė-Daugėlienė* played a key role in coordinating the Agency's support of accountability efforts for Russian crimes in Ukraine. As Na-

tional Member for Lithuania, she supported the establishment of the Joint Investigation Team (JIT) on alleged core international crimes (CICs) in Ukraine and contributed to the creation of the International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA) (→eucrim 1/2025). (CR)

New Romanian National Member at Eurojust

In May 2026, the new National Member for Romania at Eurojust, Prosecutor *Emilia Ioana Lionte,* took up her duties.

Before joining Eurojust, Ms *Lionte* served within Romania's National Anticorruption Directorate and gained extensive experience in international judicial cooperation, working as a national expert at the European Court of Human Rights (EtCHR) and, most recently, as a trial lawyer in the Office of the Prosecutor of the International Criminal Court (ICC).

Ms *Lionte* succeeds *Daniela Buruiană* as Romania's National Member at Eurojust. (CR)

Frontex

Annual Report 2025: Frontex Consultative Forum on Fundamental Rights

On 2 June 2026, the Frontex Consultative Forum on Fundamental Rights published its thirteenth Annual Report. The report outlines the main observations and recommendations shared by the Consultative Forum with Frontex and its Management Board throughout 2025.

The recommendations are aimed at strengthening the protection of fundamental rights in the Agency's activities, including a seminar on fundamental rights compliance under the EU Migration and Asylum Pact, guidance on the Frontex screening toolbox, and a position paper submitted to the European Commission on the revision of the European Border and Coast Guard Regulation. Further contributions concern advice on Frontex VEGA operations (activities focused on the identification of vulnerable persons) and revisions of relevant handbooks, fundamental rights advice from the Fundamental Rights Guidance Board (FRGB) of the European Travel Information and Authorisation System (ETIAS), and advice on fundamental rights training.

2025 saw the following developments:

- No activities were suspended or launched under Art. 46 of the Frontex Regulation (the Executive Director can take such measures in cases of serious or persistent fundamental rights violations);
- Despite general references to fundamental rights protection in operational plans, some plans still do not include operation-specific safeguards recommended by the Fundamental Rights Officer;
- Serious incident reports and reporting by international and civil society organisations continue to point to alleged serious fundamental rights violations, particularly in Greece, Bulgaria, and Serbia;
- The Forum expresses concern over the Management Board's refusal to reform the Frontex complaints mechanism, based on a proposal by the Fundamental Rights Officer to allow the direct referral of complaints involving Member State authorities to national complaints bodies, a proposal that remains pending following objections from some Member State representatives;
- The Forum reports limited progress in the handling of Frontex debriefing activities. While intended to gather intelligence, these activities continue to pose fundamental rights risks and require clearer safeguards and guidance.

In 2026, the Forum aims to assess the extent to which the Executive Director follows the advice of the Fundamental Rights Officer and introduces specific safeguards and thresholds, including conditioning Agency support on Member States' agreement to implement mitigating measures in operational plans. (CR)

Frontex and Armenia Initial New Cooperation Arrangement

During the EU–Armenia summit held on 4/5 May 2026, Frontex and Armenia formally initialled a new Working Arrangement on border and migration management.

The proposed arrangement provides for cooperation in areas including training, exchange of expertise, and risk analysis. Initialling confirms agreement on the text by both sides but does not yet create legal obligations, and the arrangement has not entered into force.

Before it can be signed, the text must still complete several approval procedures, including review by the European Commission, the European Data Protection Supervisor, and Frontex's Fundamental Rights Officer and Management Board.

The new arrangement will follow up a working arrangement concluded between Frontex and Armenia in 2012. (CR)

Frontex and EUAA Sign New Working Arrangement

On 22 January 2026, Frontex and the European Union Agency for Asylum (EUAA) signed a new Working Arrangement to support Member States by providing technical and operational assistance in the areas of migration, return, asylum, and reception. This enhanced cooperation also aims to support the implementation of European Integrated Border Management (EIBM) and the Common European Asylum System (CEAS), while improving coordination and information exchange.

This updated cooperation framework replaces the one established in 2012 between Frontex and the Europe-

an Asylum Support Office (EASO), reflecting the EASO's replacement by the EUAA and the evolution of both agencies' mandates and activities. This agreement comes ahead of the application of the EU Pact on Migration and Asylum on 12 June 2026.

Under the new Working Arrangement, cooperation between the two agencies will be strengthened in the following ways:

- Provision of more coordinated operational support on the ground, and alignment of activities such as screening and registration, asylum procedures, reception and return;
- Enhancement of systematic information sharing, including through EUROSUR, to support a common situational picture at the external borders;
- Development and use of shared analytical tools and operational products to promote consistent approaches across Member States;
- Reinforcement of preparedness by exchanging assessments, strengthening training and staff cooperation, and supporting the use of EU systems such as Eurodac.

Through closer planning and reinforced contingency measures, the agencies aim to provide more coherent EU support, avoid duplication, and optimise the use of resources. They will also collaborate closely with national authorities to implement measures related to the EU Pact on Migration and Asylum, e.g., to support the consistent rollout of new screening rules at the external borders. (CR)

Areas of Crime

Protection of Financial Interests

Deliberations on the New EU Long-Term Budget – State of Play

After negotiations on the EU's next long-term budget, the multiannual financial framework for the years 2028–2034 (MFF 2028–2034), had stalled for a time, they picked up momentum again in the spring of 2026. Whilst the European Commission has proposed a fundamental reform of the EU budget – under which, for example, fewer funds would be channelled directly to Member States for agriculture and cohesion, with more money instead being allocated to promoting the EU's competitiveness – the European Parliament (EP) and those Member States that benefit from cohesion policy and the CAP, have defended their budgets. By contrast, Member States considered „frugal", such as Germany, have been putting the brakes on increased spending. For the developments on the new MFF →eucrim 3/2025, 302–303. For the Commission's proposal →eucrim 2/2025, 136–137. The key developments in the negotiations during the last months are briefly summarised chronologically in the following:

- **17 March 2026**: At the General Affairs Council, ministers from the EU Member States hold a policy debate on the governance aspects of the MFF 2028–2034. Many Member States call for the Council to play a greater role in relation to the Commission's proposals, particularly regarding the design of programmes and strategic steering. Part of the debate are the three main funds under the next MFF, i.e., the National and Regional Partnership Plans (NRPPs), the European competitiveness fund, and the Global Europe instrument.
- **14 April 2026**: Ahead of the informal meeting of the Heads of State or Government on 23–24 April 2026, the President of the European Council, *António Costa*, sends a letter in which he called for an agreement (= general approach of the Council) on the next MFF to be reached by the end of the year. According to *Costa*, the discussion on this matter has "become more urgent" following the postponement of discussions in March. EU leaders need to discuss the appropriate level of financing to achieve the EU's ambitions (including the importance of New Own Resources) as well as the contribution of the new EU long-term budget to the EU's competitiveness agenda. The Council plans to conclude the negotiations on the MFF by the time of the presidential elections in France in April 2027.
- **28 April 2026**: The EP sets out its position for negotiations with the EU Member States on the long-term budget. MEPs propose setting the post-27 budget to 1.27 % of the EU's gross national income (excluding debt repayment costs). This would be an increase of 10% compared to the Commission's proposal of July 2025. This increase would be distributed evenly across the three budget headings supporting EU priorities (excluding administration and agencies). Overall, the EP proposes a seven-year budget of €1.78 trillion (2025 constant prices), or €2.01 trillion (current prices). MEPs plead for distinct allocations for policies under the national and regional partnership plans, including the common agricultural policy and fisheries policy, cohesion policy, the European Social Fund and home affairs. They also stress that regional and local authorities should be fully involved in planning and implementing the programmes. As detailed in another resolution (→separate news item), MEPs reiterate that simplification must not undermine transparency, accountability or democratic oversight. Lastly, the EP is calling for the introduction of new own resources, including a levy on digital services, a levy on online gambling, the extension of the Carbon Border Adjustment Mechanism (CBAM), and a levy on capital gains from cryptocurrencies.
- **6 May 2026**: The European Committee of the Regions(CoR) presents its key demands for the future MFF. Regions and cities are calling, amongst other things, for a strong and independent cohesion policy as a key instrument for promoting economic, social and territorial cohesion in the

EU. Cohesion funding should remain open to all regions and not, as proposed by the Commission, be reserved exclusively for the less developed regions. Furthermore, the CoR requests that national investment plans must be prepared in consultation with local and regional authorities. If this is not the case, regions and cities should have the right to activate a „subsidiarity clause" and notify the European Commission so that it can reject overly centralised NRPPs.

■ **14 May 2026**: On the occasion of the awarding of the Charlemagne Prize to *Mario Draghi*, German Chancellor *Friedrich Merz* calls for a "fundamental modernisation" and a "radically streamlined structure" for the next MFF. *Merz* criticises the current EU budget as outdated and too heavily focused on redistribution. In order to meet today's challenges, a modern, investment-oriented — a "Draghi-proofed" — budget is required. The chancellor makes it clear that he rejects the idea of new European debt: "Germany cannot go down this path, if only for constitutional reasons," Merz said.

■ **20 May 2026:** In a Parliament debate together with the Commission, the majority of MEPs comes out in favour of an EU-wide levy on online gambling. This is intended to serve as a new source of own resources to finance the MFF (see above). *Piotr Sarafin,* the Commissioner responsible for the EU budget, does not comment on the substance of the matter, given that the Commission is currently reviewing the proposal. However, MEPs also raised critical legal and political questions, particularly regarding the relationship with existing national taxes and the preservation of Member States' tax sovereignty.

■ **26 May 2026:** A policy debate on the next MFF 2028–2034 in the General Affairs Council focuses on the MFF's contribution to the integration of the EU's single market. Disagreements over the budget size and funding come to light. Germany continues to oppose the significant increase in the MFF proposed by the Commission, arguing that it was not financially viable. No agreement can be reached on the repayment of NextGenerationEU debt either.

■ **11 June 2026:** The Cyprus Council Presidency presents a new „negotiating box" for the MFF 2028–2034. For the first time, the Council puts forward specific figures. The Presidency proposes a ceiling for commitments of €1,730.2 billion (at 2025 prices) and a ceiling for payments of €1,733.5 billion (also at 2025 prices). This represents a moderate reduction of approximately 2% on the Commission's original proposal. The three new sources of EU own resources recently proposed by the EP (on crypto-assets, online gambling and large digital companies) are not mentioned. The future of the contribution rebates, from which Germany, amongst others, would benefit, is also left open.

■ **16 June 2026:** The two EP rapporteurs respond to the negotiating box put forward by the Cyprus Council Presidency. They reject the Council's proposal to cut the budget by 2%. Among other things, they pointed out that the appropriations for agriculture and cohesion were already at a very low level and that further cuts would further weaken the EU's ability to act.

■ **16 June 2026:** The General Affairs Council agrees on a partial general approach to the Regulation on National and Regional Partnership Plans (NRPP) as a key instrument of the EU budget for 2028–2034 (NRPP Regulation). Under the future NRPP Fund, each Member State would draw up a single comprehensive plan to replace the current separate programmes for cohesion, agriculture, fisheries, migration and security, as well as the Climate and Social Fund. The Council stresses that its approach intends to ensure appropriate flexibility for Member States when preparing and implementing their investment plans. The Council also adopts its partial negotiating position on the regulation establishing the new European Competitiveness Fund (ECF) – another central pillar of the next EU multi-annual budget – as well as on Global Europe, the EU's main financing instrument for external action for the period 2028 to 2034.

■ **19 June 2026:** The Heads of State or Government adopt conclusions on the next multiannual financial framework at the European Council. The debate brings to light the structural conflicts between the „modernisers" (Germany, Austria and the Netherlands) and the „friends of cohesion" (primarily southern and eastern European Member States). The Irish Council Presidency is called on to take the work forward on the „Negotiating Box" by the October European Council. An agreement should be reached by the end of 2026. (TW)

EP: Performance-Based Funding Should Not Be the Model for Next MFF

spot light

On 28 April 2026, the European Parliament (EP) adopted a resolution on control, transparency and traceability of performance-based instruments. It was based on an own-initiative report by MEP Monika Hohlmeier (EPP, DE), Vice-Chair of the Committee on Budgets.

In light of experiences gained from the Recovery and Resilience Facility (RRF) – the first performance-based instrument at the EU level where payments are linked to the achievement of milestones and targets rather than the reimbursement of eligible costs – the resolution raises concerns about the use of a similar model in the next multiannual financial framework (MFF) for the majority of EU financing programmes, as proposed by the European Commission (→eucrim 2/2025, 136–137).

While the resolution acknowledges that the generalised use of financing

not linked to costs may reduce the administrative burden, it also highlights that this approach increases the risk of irregularities, double funding, and fraud. Consequently, it reduces the transparency and traceability of Union funds. MEPs advocate that financing not linked to costs should only be used for smaller beneficiaries implementing projects below defined financial thresholds, while large-scale and complex projects should remain cost-based. They also insist that it should be the Commission that assesses whether milestones and targets triggering EU payments have been fulfilled.

According to the resolution, any future performance-based instrument must be accompanied by more specific key performance indicators and be harmonised from one Member State to another. Furthermore, corrective measures must be taken to strengthen audit and accreditation procedures. MEPs also make several specific recommendations for strengthening the control, transparency and accountability of performance-based instruments, such as:

- Establishing a unified accountability system that enables the traceability of EU budget contributions to specific projects and their real final beneficiaries, including contractors and sub-contractors;
- Granting financing only for measures directly linked to concrete, verifiable projects that demonstrate tangible progress and measurable results, contribute to Union policy objectives, and can be subject to effective monitoring and controls;
- Establishing a single, integrated and interoperable information and monitoring system as a precondition for accessing Union funding in the next MFF.

Ultimately, MEPs urged the Commission to implement robust safeguards to ensure the consistency, independence, and quality of audit work in all Member States. This should include the introduction of AI-powered predictive analytics tools to enable auditors to assess risks in real time and detect anomalies more effectively. (TW)

ECA Opinions on Next MFF: "Many Changes May Not Make the Budget Better"

In the first quarter of 2026, the European Court of Auditors (ECA) published a dozen opinions on the various EU programmes for the next Multiannual Financial Framework (MFF 2028–2034), as proposed by the European Commission in July and September 2025 (→eucrim 2/2025, 136–137). These opinions are available in all 24 EU languages on a dedicated ECA website.

On 28 April 2026, the ECA published an overview document summarising common features and lines of argument included in the different opinions. While the ECA stresses that each opinion must be read independently, overall it concludes that „many changes to the EU's long-term budget may not actually make it better".

The overview document outlines the timeline and context of the next MFF and summarises the major changes compared to the current MFF. It also outlines the key risks and challenges identified, which are grouped under eight thematic areas:

- **Financing the EU budget**: There will be a significant budget shortfall if the proposed revenue streams are not approved. Furthermore, the large amount of planned new borrowing could require Member States to make additional national contributions to service the debt, even in a strained budgetary situation;
- **EU added value**: The Commission has missed the opportunity to define how EU spending adds value beyond national spending alone;
- **Aligning spending objectives with EU priorities**: Leaving spending priorities largely in the hands of Member States with diverging interests will make it difficult to address EU-level objectives;
- **Simplification**: The plan to reform shared management would shift administrative burdens from the Commission to Member States and beneficiaries;
- **Budget flexibility**: Flexibility may reduce budget predictability, which is a concern for long-term investments;
- **Compliance, transparency, accountability, and traceability of spending**: The proposed assurances and accountability arrangements are too reliant on Member States, whose national control systems have often proved weak;
- **Performance work**: The proposed framework has a weak design; it will be difficult to measure the results of EU spending and what EU citizens ultimately get for their money. In addition, it is not ensured that Member States adequately report performance information to the Commission;
- **ECA mandate**: The proposals are not sufficiently clear in giving the ECA unrestricted rights to access information and information systems.

The ECA also stressed that large parts of the Commission proposal are inspired by the outgoing Recovery and Resilience Facility model, for which the ECA identified several shortcomings in relation to accountability and control. Even though some of the ECA's issues have been addressed, others remain unresolved, particularly the need to focus on results rather than outputs and to establish a clear link between funding and results. ECA's opinions will feed into the negotiations among the policy-makers (European Parliament and Council) who will decide on the next seven-year MFF. (TW)

AG: Associations Can Bring Annulment Actions against RRF Approval

spot light

In her Opinion of 16 April 2026 in Case C-555/24 P (*Medel and Others v Council*), Advocate General (AG) *Tamara Ćapeta* proposed that associations representing judges

have standing to bring actions for annulment against the Council's decision approving justice system milestones concerning Poland under the EU Recovery and Resilience Facility (RRF).

➤ *Background of the case*

The General Court (GC) dismissed actions brought by four associations active in defending judicial independence, which sought annulment of the Council implementing decision approving Poland's recovery and resilience plan (Joined Cases T-530/22 to T-533/22). They argued that the conditions for the disbursement of funds did not comply with EU law, whereby three milestones concerned the Polish justice system. The GC found that the applicant organisations are not entitled to bring proceedings either in their own name or on behalf of the judges whose interests they defend. Neither did the RRF Regulation grant that procedural right nor are the judges/associations directly concerned by the Council decision.

➤ *The Advocate General's Opinion*

AG *Ćapeta* believes that the GC erred in law with regard to two aspects:

- Milestones F2G and F3G, which specifically obliged Poland to introduce review proceedings for disciplinary sanctions imposed on judges by the Disciplinary Chamber of the Polish Supreme Court, directly concern at least those judges who were affected by the disciplinary decisions;
- In the light of the principle of effective judicial protection, associations may challenge EU acts affecting their own interests.

With regard to the latter context, AG *Ćapeta* discusses the broader issue of when associations acting in their own name may be directly and individually concerned within the meaning of Art. 263(4) TFEU. In the case of an association acting in its own interest, she suggests that „*direct concern*" should be understood as requiring that „the challenged act is a direct source of the effects on the collective interests that the association defends." The condition of „*individual concern*" should relate to whether the association's „core interests and activities differentiate it from other associations and from its members in relation to the challenged measure". The AG clarifies that, „in that respect, it does not matter that the association at issue is not the only one protecting the collective interests; it only needs to be identifiable through the collective interests that are involved in a case."

Applying these definitions, the AG considers that the applicant organisations whose purpose is to safeguard the independence of the judiciary in Poland, have standing in their own name for the purposes of bringing actions for annulment to challenge milestone F1G. This milestone requires measures to strengthen the independence of the Polish judiciary.

In conclusion, AG *Ćapeta* considers that a part of the grounds of appeal are well-founded, and thus the actions for annulment in the present case are admissible. She proposes that the case be referred back to the GC for a decision on the merits. (TW)

AG: The Commission Was Not Allowed to Release Funds for Hungary

spot light

In her Opinion, published on 12 February 2026 in Case C-225/24 (*Parliament v Commission*), Advocate General (AG) *Tamara Ćapeta* proposes that the Commission's decision to release EU funds withheld from Hungary be annulled.

➤ *Background of the case*

On 13 December 2023, the European Commission took a decision (which remained unpublished) to authorise the disbursement of approximately €10.2 billion to Hungary, after these funds had been withheld due to infringements of EU law under the Common Provisions Regulation (Regulation (EU) 2021/1060). This Regulation sets out the common financial rules that apply to a number of sources of EU funding for the period 2021–2027. Pursuant to the so-called enabling conditions, EU Member States must, *inter alia*, ensure fundamental rights are respected and the Charter of Fundamental rights of the European Union (CFR) is complied with (→*Jaskolska*, eucrim 4/2023, 337–339). In 2022, the Commission suspended the disbursement and required Hungary to fulfill several conditions to comply with the CFR, including the independence of the judiciary. In its 2023 decision, the Commission concluded that Hungary had satisfied the requirements of the CFR in relation to judicial independence and lifted the suspension (→eucrim 4/2023, 311 and *Kuhl*, eucrim 4/2023, 339–345).

The European Parliament brought an action against this decision in March 2024 (→eucrim 1/2024, 6). It argued that the Commission infringed the applicable law and committed manifest errors of assessment, infringed its duty to state reasons and misused its powers.

➤ *The AG's Opinion*

According to AG *Ćapeta*, the European Commission did not sufficiently verify that Hungary had met the requirements it had set for the release of funds. Disbursement of EU funds can only take place if the required legislative reforms are in force and are effectively being applied in the Member State concerned. The Commission must carry out a proper assessment of the reforms. In the case at issue, the Commission has not been sufficiently demonstrated that the reforms would safeguard the independence of the judiciary (in particular the Hungarian Supreme Court, the Kúria), ensure the proper appointment of judges, and remove the obstacles to requests for preliminary rulings to the Court of Justice of the EU. The Commission did also not adequately address the legislative developments that could undermine or offset the objectives of the reforms Hungary had undertaken.

Furthermore, the Commission had failed to provide sufficient grounds for its decision, contrary to Art. 296 TFEU.

Finally, the AG considered that there was insufficient evidence to support Parliament's allegation that the Commission had misused its discretion by releasing EU funds in exchange for the government under *Viktor Orbán* lifting its veto on important and urgent decisions in the Council of the European Union. (TW)

ECA Unsatisfied with Transparency and Traceability in RRF

The European Court of Auditors (ECA) has published several critical opinions and reports on the design, control framework, and implementation of the EU's Recovery and Resilience Facility (RRF) – the EU's flagship fund designed to contribute to the EU's economic recovery from the corona pandemic and to stimulate investment and reform. Under the RRF, EU Member States receive funding upon the successful completion of pre-agreed milestones and targets, which correspond to different stages in the roll-out of reforms and investments. The ECA's statements on the RRF are compiled under a dedicated website. For the recent report on the RRF scheme to tackle fraud →related link.

In its Special Report 14/2026, published on 6 May 2026, the ECA is now taking a closer look on whether the traceability of RRF funding and the transparency in the use of funding have sufficiently been ensured by the Commission and the Member States. ECA's audit findings are based on interviews with the Commission, audit visits to ten Member States (Austria, Bulgaria, Estonia, France, Germany, Latvia, Malta, the Netherlands, Romania, and Spain), a survey of all Member States, and desk research. The ECA's main findings are:

- The regulatory framework includes specific requirements for the traceability of funds and the Member States generally comply with these. However, not all countries systematically collect the required data; in some cases, countries only collect the data upon request. This results in delays and jeopardises accountability and analysis.
- A major concern is that the Commission does not collect data on actual amounts paid for individual RRF measures, even when Member States possess such data. This lack of information undermines the Commission's ability to assess the efficiency with which Member States have used the RRF funds. Moreover, Member States do not systematically use actual costs to update estimates, which leads to flaws in the reallocation of savings and in assessing whether EU funding is reasonably close to actual costs.
- Regarding transparency, the ECA acknowledges that the Commission and the Member States publish information in line with RRF rules, and provide adequate transparency regarding the achievement of milestones and targets. However, the ECA identifies shortcomings in that this information is insufficient in respect of final recipients, actual costs and results. Furthermore, the list of the 100 largest final recipients fails to properly capture the overall use of the money.

The ECA calls on the negotiators of the next multiannual financial framework, which is inspired by the RRF spending model of „financing not linked to costs", to take the findings on traceability and transparency into account. It recommends that the future framework includes provisions to ensure the comprehensive, systematic, and timely collection and publication of information on the use of EU funds. In addition, Member States should be required to systematically collect and report to the Commission actual cost data for the purposes of managing the funds, ensuring the efficient distribution of resources during implementation, and *ex post* assessment of efficiency. (TW)

ECA: EU's COVID-19 Recovery Fund Remains Vulnerable to Fraud

spot light

The Special Report 06/2026 by the European Court of Auditors (ECA), published on 11 February 2026, indicates that the Recovery and Resilience Facility (RRF) continues to suffer from weaknesses in the detection, reporting and correction of fraud cases.

The ECA's audit assessed the effectiveness of systems established by the Commission and in four EU Member States (Denmark, Spain, Italy and Romania) for the RRF to safeguard the EU's financial interests from fraud. The ECA's criticism focuses on three main issues:

- The Commission's limited verification work;
- Remaining weaknesses in Member States regarding fraud detection;
- Undermined protection of the EU's financial interests due to incomplete RRF fraud data and gaps in recovery rules.

In detail, the ECA found, for instance, that Regulation (EU) 2021/241 establishing the RRF set high-level requirements for the Member States' anti-fraud systems, but did not sufficiently detail them. Although the Commission attempted to rectify the situation by introducing stricter requirements in the financing agreements, the requirements for national controls remained unclear.

The ECA acknowledged that the Commission's audits contributed to improved anti-fraud systems of the assessed Member States. However, these audits have still weaknesses, such as insufficient coverage of the audit body and the anti-fraud responsibilities of the coordinating body. Another shortcoming is that, in some Member States, the Commission's audits were only concluded after the first payment request, leading to payments without sufficient evidence about the effectiveness of the Member State anti-fraud control system.

Looking at anti-fraud prevention measures in the Member States, the ECA found that all selected states had established anti-fraud policies, but these were often delayed. In addition, key fraud detection measures, such as desk and on-the-spot checks, and whistleblowing channels, have shortcomings. In particular, many countries underused the potential of data mining and analytics.

With regard to procedures, the ECA found that there is no standard to report fraud cases to the Commission and Member States apply different criteria on what constitutes RRF fraud. As a consequence, it is difficult for the Commission to properly target its own anti-fraud action and to accurately estimate the extent of RRF fraud.

Ultimately, the ECA points out that Member States are only required to take legal action to recover funds while other EU funds use a wider range of corrective actions, such as the withdrawal of projects or the suspension of payments. Contrary to other EU funds, Member States are, in principle, also not required to return recovered funds to the EU budget. As many fraud cases may emerge after the end of the RRF, the appropriate recovery remains uncertain as reporting and anti-fraud mechanisms come to an end as well.

The ECA makes several recommendations to the Commission and the Member States, including:

- Further strengthening of Commission checks of national RRF anti-fraud systems;
- Improving Member State reporting of suspected fraud in the RRF, which should include respective guidance by the Commission;
- Increasing the impact of corrective measures;
- Defining minimum anti-fraud requirements for EU countries.

These recommendations are designed to be adopted in future RRF-type programmes, in which payments are not linked to actual costs. (TW)

Governance and Innovation for Fraud Prevention in EU Agricultural Funds – The GINGER Project

GINGER – **G**overnance and **IN**novation for **G**enerating **E**ducation and **R**egularity in EU agricultural funds – is a 24-month project co-funded by the European Union under the **Union Anti-Fraud Programme (EUAF-2025-TRAI-02)** and coordinated by **UnitelmaSapienza University of Rome**. The project is also developed in institutional collaboration with the Guardia di Finanza – Unit for the Repression of Fraud against the European Union, operating within the Department for European Affairs of the Presidency of the Council of Ministers and serving as the Technical Secretariat of the Italian AFCOS. Running from March 2026 to February 2028, GINGER aims to strengthen fraud prevention and governance in the management of Common Agricultural Policy (CAP) funds through capacity building, innovation and transnational cooperation.

The project addresses persistent challenges in CAP fraud prevention, including uneven detection capacities, fragmented information exchange and different levels of digital readiness across Member States. Particular attention is given to fraud risk analysis and the application of AI, machine learning and big data analytics to CAP fund management and control. More information is available at the project website.

GINGER is structured around **10 international events** bringing together public authorities, Anti-Fraud Coordination Services (AFCOS), paying agencies, EU institutions, academia and private-sector stakeholders to exchange practices and develop data-driven approaches to fraud prevention. Participation is **open to all interested participants**, and all events are accessible online, including those hosted in person. A certificate of attendance is provided for each event.

Through training, peer learning, risk-mapping and collaborative activities, the project will progressively develop the **GINGER Learning Package**, consolidating the knowledge and methodologies generated throughout the project into practical resources for future training and capacity-building initiatives.

The first two events have already taken place, and the third event entitled "From Red Flags to Risk Maps: AI and Big Data for Early Warning", will be held **online on 21 September 2026**. Registration is already open: <https://forms.gle/hXyeuGw9VDH2Ed6g7>

Further information on the project, including the complete overview and schedule of upcoming events, presentations, recordings and other materials from completed activities, is available in the dedicated GINGER dissemination folder: <https://drive.google.com/drive/folders/1fhgqj8jO-sUtZ-jCfk46A3BGEiASYlmcC?usp=drive_link>.

For information on upcoming events, inclusion in the GINGER mailing list, or to express interest in contributing as an **expert or speaker and/or involving your organisation in the project network, please** contact ginger.project@unitelmasapienza.it.

Project updates are also available on LinkedIn: **@GINGER – EU Funds Governance & Innovation**.

(Maria Virginia Sirolli)

Tax Evasion

EDPS Opinion on EPPO's and OLAF's Access to VAT Information

On 8 January 2026, the European Data Protection Supervisor (EDPS) published his opinion on the legislative proposal to amend Regulation 904/2010, which would grant the European Public Prosecutor's Office (EPPO) and the European Anti-Fraud Office (OLAF) specific direct and centralised access to VAT information at EU level (→eucrim 3/2025, 204–205).

The EDPS welcomes the objectives of the proposal and recognises that EPPO's and OLAF's direct access to VAT information is necessary to achieve the objective to effectively combat intra-Community VAT fraud. He stresses, however, that the proposal is at the sensitive crossroads between administrative VAT cooperation and criminal law enforcement. Data protection follows different legal regimes and principles in these fields, which is why the separation must be carefully reflected in the legal framework.

The EDPS recommends that the proposal more clearly explains and underlines the exceptional nature of providing direct (albeit limited) access to administrative databases for law enforcement purposes. In addition, it should be clarified to avoid that the envisaged amendments would be misconstrued or later relied upon as precedent for more general application.

The EDPS also emphasises that appropriate legal, technical and organisational safeguards tailored to the targeted nature of the measure are needed. While some technical and organisational details may be specified through implementing acts (as envisaged by the proposal), core parameters must already be defined in the basic legislative act. Therefore, the EDPS recommends the inclusion of several additional safeguards in order to comply with the EU data protection law principles, such as purpose limitation, data minimisation and accountability. (TW)

Tax Blacklist: Council Adds Two Additional Countries

Twice a year, the Council decides which countries and territories are to be blacklisted as non-cooperative tax jurisdictions (for the last decision in October 2025 →eucrim 3/2025, 205–206).

On 17 February 2026, the Council added two countries – the Turks and Caicos Islands and Vietnam – to the EU list of non-cooperative jurisdictions for tax purposes. At the same time, it removed three countries – Fiji, Samoa and Trinidad and Tobago – from the list, as they now meet all agreed international standards. This list now comprises 10 jurisdictions: American Samoa, Anguilla, Guam, Palau, Panama, the Russian Federation, the Turks and Caicos Islands, the US Virgin Islands, Vanuatu and Vietnam.

In addition, the Council approved the progress report (Annex II), which documents cooperation with partner countries and their commitments to reforming their tax regulations. Antigua and Barbuda and the Seychelles will be removed from the document

Strengthening the Protection of EU's Financial Interests via Criminal Law

The research project, led by Prof. *Anna Maria Maugeri* at the University of Catania, aims to strenghten the consolidation of the protection of the EU's financial interests through a systematic analysis of the legislation on fraud, corruption, money laundering, and the liability of legal persons. The uneven implementation of EU regulatory tools creates different levels of protection for the EU's financial interests, which puts the Union's budget and the credibility of its institutions at risk.

Therefore, the study will assess the effectiveness and level of implementation of legal instruments, such as Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law (the "PIF Directive") as well as Council Regulation (EC, Euratom) No. 988/95 covering checks in EU countries and the imposition of penalties in the event of irregularities. Other instruments to be assessed include Directive (EU) 2026/1021 on combatting corruption; the EU legislation on anti-money laundering; and Directive (EU) 2024/1260 on asset recovery and confiscation. Additionally, the research covers the activities of the European Public Prosecutor's Office (EPPO) in prosecuting PIF crimes.

The project consists of the following main steps:

- Review of the EU's legal frameworks aimed at safeguarding the Union's financial interests, concentrating on specific Member States and the EPPO's jurisdiction over material matters (March – August 2025);
- Assessment of the EU's legal mechanisms to tackle corruption that damages the EU's financial interests (September 2025 – February 2026);
- Examination of anti-money laundering (AML) policies at both EU and national levels to secure the EU's financial interests (March – August 2026);
- Review of corporate liability systems in combating fraud, corruption, and money laundering within selected Member States, emphasizing the protection of the EU's financial interests (September 2026–February 2027);
- Exchange of knowledge, formulation of policy advice, and dissemination of the project's results (August 2025 – February 2027).

The research team at the Centro di Diritto Penale Europeo at the University of Catania has already achieved some significant results, including scientific publications in high-ranking law journals and an online workshop entitled "Protecting EU Financial Interests: EU Legal Instruments and their National Implementation in Selected Member States", as well as an international conference in Catania entitled "Strengthening the Protection of the EU's Financial Interests via Criminal Law: Fraud Prevention and Anti-Corruption Measures".

This project is co-funded by the European Union Anti-Fraud Programme (EUAFP, [GA no. 101193934]).

To find out more about the project and its results, visit: https://pifitalia.lex.unict.it/

(Amalia Orsina)

following a positive assessment of their exchange of information. Brunei has been granted a six-month extension to bring its tax regulations into line and will also be removed from the list.

The criteria for blacklisting non-cooperative jurisdictions relate to tax transparency, fair taxation, and measures against base erosion and profit shifting. If a country is blacklisted, EU Member States are required to take efficient defensive measures in non-tax and tax areas (→eucrim 3/2023, 255–256). (TW)

Corruption

Directive on Combatting Corruption Adopted and Published

spot light

In spring 2026, the European Parliament and the Council reached an agreement on the text of the Directive on Combatting Corruption, concluding a lengthy negotiation process. Proposed by the Commission on 3 May 2023, the Directive aims to harmonise criminal law relating to corruption offences, enhance the prevention of corruption, and improve law enforcement cooperation (→eucrim 2/2023, 140–141). The Directive was published in the EU's Official Journal 2026/1021 on 11 May 2026.

Directive (EU) 2026/1021 harmonises the definition of corruption offences across EU Member States (except Denmark, which is not bound by the Directive) – going beyond the offence of bribery. The minimum level of criminal penalties is also harmonised for both individuals and companies. The Directive also contributes to making the investigation and prosecution of corruption more effective, and includes provisions aimed at strengthening preventive and integrity measures in Member States. For example, the Directive foresees the adoption of national anti-corruption strategies by Member States.

Member States will have 24 months to transpose the Directive into national law. An exception applies to the provisions on risk assessments and national strategies, for which the deadline is 36 months. The following Q&A summarises the Directive's main features.

➤ *Why does the new anti-corruption Directive matter?*

For the first time, the bloc has established a more coherent EU-wide anti-corruption framework. Earlier rules were piecemeal and resulted in significant variation among Member States. Directive (EU) 2026/1021 seeks to align criminal offences, penalties, corporate liability, prevention measures and enforcement capacity. Its primary purpose is to tackle corruption by means of criminal law, enabling better cross-border cooperation between competent authorities. The Directive also seeks to amend and expand the provisions of existing EU anti-corruption instruments.

➤ *What will happen to the existing criminal anti-corruption instruments?*

Currently, the EU's anti-corruption efforts were based on Council Framework Decision 2003/568/JHA, which sets out requirements for the criminalisation of corruption in the private sector, and a 1997 convention addressing certain acts of corruption involving European Community or Member State officials. These instruments will be replaced in their entirety in relation to the Member States bound by the new Directive. As Ireland declared its wish to take part in the application of the Directive, only Denmark will not be bound by it and will continue to apply the „old" framework.

➤ *What is new from a European criminal law perspective?*

The Directive harmonises a core set of corruption-related offences across the EU. It is not limited to classic public-sector bribery. It extends to:

- Active and passive bribery;
- Corruption in both the public and private sectors;
- Misappropriation or diversion of property by public officials;
- Trading in influence;
- Unlawful exercise of public functions;
- Obstruction of justice;
- Enrichment from corruption offences;
- Concealment.

The harmonisation of specific offences with a broad definition of the elements of crime is aligned with deliberately broad concepts of „public official" and „undue advantage". Thus, the Directive will considerably broaden and standardise the EU Member States' substantive criminal law landscape.

The Directive also establishes secondary liability for Directive offences (incitement as well as aiding/abetting, except for the unlawful exercise of public functions). Member States must criminalise attempted enrichment and concealment, and may also criminalise attempted bribery, misappropriation and trading in influence.

➤ *How does the Directive address legal persons?*

Member States are obliged to ensure that legal persons can be held liable where corruption offences are committed for their benefit by persons in leading positions, or where inadequate supervision or control enabled the offence. The Directive acknowledges the implementation of genuine, effective and duly assessed internal controls, ethics and compliance programmes as a mitigating circumstance, whether these were established prior to or after the offence. Lower penalties may also be considered if a legal person swiftly discloses information and takes remedial measures. The Directive clarifies, however, that the fact that the legal person has compliance programmes only for cosmetic purposes (called "window dressing") should not amount to a mitigating circumstance. Consequently, the Directive links anti-corruption enforcement to governance fail-

ures, requiring companies to prove the effectiveness of their compliance programmes if they wish to defend themselves against a corruption offence.

➤ *How does the Directive harmonise penalties?*

The Directive distinguishes between penalties for natural persons and those for legal persons.

Member States must provide effective, proportionate and dissuasive penalties, including imprisonment for natural persons. It sets minimum standards for maximum penalties for the main offences, and also contemplates additional sanctions, such as fines, removal or suspension from public office, disqualification and exclusion from access to public funding, including tender procedures, grants, concessions and licences.

For legal persons, the Directive requires the imposition of fines based on worldwide turnover or fixed maximum amounts. The maximum level of such fines is to be graded according to the type of corruption offence in the Directive, i.e.:

- For bribery (public and private) and misappropriation (Arts. 3–5 of the Directive): 5% of total worldwide turnover or an alternative fixed amount of €40 million;
- For trading in influence, obstruction of justice and enrichment (Arts. 6, 8 and 9 of the Directive): 3% of total worldwide turnover or an alternative fixed amount of €24 million.

Beyond fines, the Directive authorises additional corporate sanctions depending on the gravity of the conduct, including:

- Exclusion from public benefits, aid and funding (including tenders, grants, concessions and licences);
- Temporary or permanent disqualification from business activities;
- Withdrawal of permits;
- Contract annulment or rescission;
- Placement under judicial supervision;
- Judicial winding-up;
- Closure of establishments used to commit the offence.

➤ *What other criminal law provisions are included in the Directive?*

The Directive sets out the aggravating and mitigating circumstances that national law should implement when sentencing offenders (see also above Q on how legal persons are addressed). It also obliges Member States to establish that privileges with regard to and immunity from investigation and prosecution granted to national officials for offences referred to in this Directive can be lifted. Furthermore, the Directive includes obligations for establishing jurisdiction and penalty-tier-based limitation periods (see Arts. 18 and 19 of the Directive for details).

➤ *What is the Directive's preventive dimension?*

This is one of the instrument's most significant aspects, as the Directive not only criminalises certain acts, but also calls for Member States to establish or maintain anti-corruption frameworks that include:

- Integrity policies;
- Risk assessments;
- Conflict-of-interest rules;
- Transparency mechanisms;
- Ethics and training measures;
- Safeguards in procurement and public decision-making.

➤ *How should transparency and integrity in public life be strengthened?*

The Directive also emphasises the need for civil society, independent experts, researchers and other stakeholders to be increasingly involved in the development of national anti-corruption efforts. Member States have also an obligation to guarantee an enabling environment for journalists, protect their safety, and proactively promote media freedom and pluralism, since (investigative) journalism plays an important role in scrutinising public affairs, detecting possible corruption and integrity breaches, raising awareness, and promoting integrity. Member States may also wish to consider ensuring that „members of the public concerned" are represented in criminal proceedings in corruption cases.

➤ *How are the capacities of the authorities in the Member States leveraged?*

The Directive obliges Member States to have in place bodies or organisational units tasked with the prevention and repression of corruption. Preventive tasks can include assessing the asset declarations of national officials, as designated by national law; monitoring compliance with transparency or conflicts of interest rules; and identifying sectors or occupations most at risk of corruption. Member States must also ensure that resources and powers allocated to such bodies or organisational units are commensurate with the proper administration of their tasks and allow for specialised knowledge of the prevention and repression of corruption.

➤ *How is coordination and cross-border cooperation improved?*

According to Art. 32 of the Directive, the competent authorities of the Member States concerned shall consider referring information related to suspected cross-border corruption offences to appropriate competent Union institutions, bodies, offices or agencies.

The Member States, Europol, Eurojust, the EPPO and OLAF and the Commission shall, within their respective competences, cooperate with each other in the fight against the criminal offences referred to in this Directive. To that end, Eurojust shall, where appropriate, provide the technical and operational assistance needed by the competent authorities to facilitate coordination of their investigations. The Commission and OLAF may, where appropriate, provide assistance.

In addition, the Commission shall facilitate cooperation through the EU network against corruption (see Art. 33 of the Directive for further details).

Lastly, Member States must ensure that information is exchanged between competent law enforcement authorities using Europol's Secure Information Exchange Network Application (SIENA) (Art. 28 of the Directive).

➤ *Is the PIF Directive affected by the new Corruption Directive?*

Yes. To provide for an equivalent level of protection between the Union's and the national financial interests, the provisions of Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law (the PIF Directive) are aligned with those of Directive 2026/1021. To this end, the rules applicable to criminal offences affecting the Union's financial interests as regards criminal or non-criminal penalties, aggravating and mitigating circumstances, and limitation periods are amended by the new Directive (see Art. 36 of Directive 2026/1021 for details). See also the article by L. Zoli, „The Amendment of the PIF Directive by the New Proposal for a Directive on Combating Corruption", (2023) eucrim, 279–281.

➤ *What are the likely implications for Member States?*

Member States will need to examine whether their laws and institutions meet the new requirements in several areas:

- The scope of criminal offences;
- Sanctions levels;
- Legal person liability;
- Confiscation tools;
- Anti-corruption prevention policies;
- Institutional capacity and cooperation mechanisms.

For some jurisdictions, the main changes may concern penalties or corporate liability, while for others, the greater challenge may lie in prevention and institutional architecture.

➤ *What does the Directive mean for companies?*

Companies should expect heightened scrutiny of:

- Third-party and intermediary relationships;
- Gifts and hospitality;
- Procurement interactions;
- Accounting and record-keeping;
- Internal controls;
- Management oversight.

The Directive's rules on legal person liability make effective compliance systems more important, especially where failure of supervision may trigger liability.

➤ *What is the broader significance of the Directive for EU criminal law?*

The Directive illustrates a broader trend in EU criminal policy, moving from isolated offence-based harmonisation towards more comprehensive governance frameworks. It connects criminalisation with prevention, administrative integrity, asset recovery and enforcement capacity. In this respect, it is a notable example of the EU's increasingly systemic approach to crime control in areas with strong implications for the rule of law. (TW)

Money Laundering

Football Enters EU Anti-Money Laundering Framework

On 27 April 2026, in an interview with Italian outlet "Calcio e Finanza", the Chair of the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), *Bruna Szego*, outlined the rationale for bringing professional football clubs and agents under the EU's anti-money laundering framework from July 2029.

Football's inclusion stems from the 2024 EU anti-money laundering package, which expanded the scope of obliged entities beyond traditional financial actors to include selected non-financial sectors deemed exposed to money laundering risks (→eucrim 2/2024, 117–118). According to the AMLA Chair, the decision to include football reflects both the scale of the football industry and its structural vulnerabilities to illicit financial flows.

The European Parliament played a key role in adding football to the final legislative package, citing concerns over the sector's global reach, large financial flows, and cross-border transactions. Ownership structures in football are often complex and not always transparent, making it difficult to identify beneficial owners and trace the origin of funds.

The economic significance of football has grown into a global industry, with major revenues generated through media rights, sponsorships, and transfers. At the same time, the sport's popularity and social visibility can make it attractive for the laundering of illicit proceeds, including through the acquisition of clubs, transfer market activity, and sponsorship arrangements.

Szego highlighted that a recurring concern is the lack of uniform regulation on the financial statements of football clubs across the EU. While some Member States already apply anti-money laundering obligations to parts of the football sector, rules remain fragmented, creating inconsistencies in supervision and oversight. The new EU framework aims to address this by establishing a harmonised set of requirements and a common risk-based methodology across all Member States.

Under the new system, clubs and agents will be required to implement customer due diligence and transaction monitoring procedures, including checks on beneficial ownership and the origin of funds. The objective is not to impose identical supervisory models across sectors, but to ensure consistent standards and a level playing field within the EU. Football will be assessed under a dedicated risk-based methodology for the non-financial sector, reflecting the specific characteristics of the industry. While AMLA will not directly supervise clubs, it will guide and evaluate the national authorities responsible for enforcement.

Overall, the interview demonstrated that the inclusion of football reflects a broader shift in the EU's anti-money laundering framework towards addressing high-risk sectors characterised by large cross-border financial flows, complex ownership structures, and significant regulatory fragmentation. (CR)

ECJ: Prior Accusation of a Natural Person Not Required to Penalise a Legal Person for AML Breaches

spot light

On 29 January 2026, the ECJ delivered its judgment in Case C-291/24, *Steiermärkische Bank und Sparkassen and Others*. In the first place, the Court clarified the conditions under which legal persons may be held liable for breaches of the anti-money laundering obligations laid down in Directive (EU) 2015/849 (the 4th Anti-Money Laundering (AML) Directive). The Court held that the Directive precludes national rules under which a legal person may be penalised only if a named natural person has first been formally treated as an accused person and found to have committed an unlawful and culpable offence attributable to that legal person. In the second place, the Court held that the Directive does not preclude national limitation periods of three years for bringing proceedings and five years for imposing a penalty, provided that the principles of equivalence and effectiveness are respected.

➤ *Background of the case and questions referred*

The request for a preliminary ruling arose from proceedings before the *Bundesverwaltungsgericht* (Federal Administrative Court, Austria) concerning an administrative criminal penalty imposed on Steiermärkische Bank und Sparkassen AG by the Austrian Financial Market Authority for breaches of its anti-money laundering due diligence obligations.

The penalty was based on §35(1) and (2) of the Austrian *Finanzmarkt-Geldwäschegesetz* (FM-GwG), under which a legal person may be held liable where a breach is committed for its benefit by a person holding a leading position within it or where that person's lack of supervision or control enables a subordinate to commit such a breach.

Two features of the Austrian legal framework gave rise to the reference. Firstly, the case law of the *Verwaltungsgerichtshof* (Supreme Administrative Court, Austria) introduced additional requirements for holding a legal person liable for an administrative fine. Accordingly, a legal person may only be penalised if: (1) the natural person whose conduct is attributed to it has been made a party to the proceedings and treated as an accused person, with all the rights attached to that status; (2) the operative part of the penalty decision identifies that person by name, establishes that he/she committed an unlawful and culpable offence; and (3), in that operative part, this offence is attributed to the legal person concerned.

Secondly, § 36 FM-GwG lays down a three-year limitation period for bringing proceedings and a five-year period for imposing a penalty, both calculated from the date on which the offence ended. Given the complexity of such proceedings and the often opaque nature of the underlying facts, the referring court questioned whether these time limits were compatible with the principle of effectiveness.

Accordingly, the referring court asked, in essence, whether Arts. 58–60 of Directive 2015/849, read in the light of the principle of effectiveness:

- Preclude the additional requirements imposed by Austrian case law for penalising legal persons;
- Preclude the limitation periods laid down in § 36 FM-GwG.

➤ *The ECJ's reasoning on the conditions for the liability of legal persons*

At first, the ECJ referred to Art. 58(1) of Directive 2015/849, which requires Member States to ensure that *obliged entities* can be held liable for breaches of the national provisions transposing the Directive. Given that Art. 2(1) of the Directive expressly includes both natural and legal persons within the definition of obliged entities, the Court inferred that legal persons must be capable of incurring liability in their own right.

It further emphasised that nothing in Art. 58 indicates that the liability of a legal person is dependent on a prior determination, in the same proceedings, that an identified natural person is personally responsible for the infringement. In support of this interpretation, it relied on two arguments derived from the overall scheme of the 4th AML Directive:

- Art. 58(3), which requires sanctions and measures to be applied against members of the management body and other natural persons responsible for the breach, submits that their liability is merely "ancillary and additional" to that of the legal person; therefore, this liability of natural persons complements, rather than conditions, the liability of the legal person.
- Art. 60(5) and (6), which define the circumstances in which the conduct of natural persons may be attributed to a legal person, presuppose that the legal person itself is capable of incurring liability. Accordingly, the legal person's responsibility depends on whether the conditions for attribution are satisfied, rather than on a prior determination that the natural person concerned is personally culpable for the infringement.

Next to this contextual interpretation, the same conclusion can be drawn from a teleological interpretation of Art. 58(1) of the Directive, which requires sanctions for breaches of anti-money laundering obligations to be effective, proportionate and dissuasive. In this context, requiring a specific natural person to be formally accused as well as found to have act-

ed unlawfully and culpably would risk undermining the effectiveness and deterrent effect of sanctions imposed directly on legal persons in their capacity as obliged entities with independent liability.

Lastly, the minimum-harmonisation character of Directive 2015/849 does not justify the Austrian approach either. Although Member States remain free to adopt stricter preventive measures and provide for additional penalties, they cannot introduce conditions that restrict the liability of legal persons required by Art. 58(1). Minimum harmonisation permits national law to exceed the level of protection prescribed by the Directive, but not to fall below it. Otherwise, national law could define the conditions for penalising legal persons so narrowly that the liability expressly required by Art. 58(1) would rarely, if ever, arise.

It is for the referring court, in accordance with the principle of consistent interpretation, to interpret the relevant national provisions, so far as possible, in the light of the wording and purpose of the Directive.

➤ *The ECJ's reasoning on the limitation periods*

Regarding the limitation periods, the ECJ observed that Directive 2015/849 does not harmonise the national rules governing the time limits for bringing proceedings and imposing penalties for breaches of anti-money laundering obligations. Member States therefore retain procedural autonomy, provided that the principles of equivalence and effectiveness are respected. Accordingly, national rules must not be less favourable than those applicable to comparable domestic proceedings, nor must they render the enforcement of rights and obligations arising under EU law practically impossible or excessively difficult.

Applying these principles, the Court recalled that reasonable limitation periods are compatible with EU law, as they serve the interests of legal certainty and the stability in legal relations. It therefore held that limitation periods of three years for initiating proceedings and five years for imposing a penalty are, in principle, consistent with EU law, observing that nothing in the material before it indicated otherwise.

➤ *Put in focus*

The judgment draws a clear distinction between the attribution of conduct to a legal person and the personal liability of the natural person concerned. Although the liability of a legal person remains dependent on the attribution criteria laid down in Art. 60(5) and (6), it does not require the prior prosecution or conviction of an identified individual in the same proceedings. Corporate liability under Directive 2015/849 is therefore autonomous, but not detached from the acts or supervisory failures of natural persons. In this respect, the ECJ continues the approach developed in *Deutsche Wohnen* (→eucrim 4/2023, 329–330), confirming that national procedural requirements must not undermine the effective and dissuasive penalisation of legal persons acting as obliged entities. At the same time, the judgment preserves Member States' procedural autonomy by accepting reasonable national limitation periods. (JK)

ECJ: Italian Trust Mandates May Be Subject to Beneficial Ownership Transparency Rules

On 21 May 2026, the ECJ delivered its judgment in Joined Cases C-684/24 and C-685/24 (Across Fiduciaria SpA and Others), concerning the application of EU anti-money laundering transparency requirements to Italian trust mandates (mandati fiduciari), particularly with regard to the reporting and disclosure of beneficial-ownership information.

Unlike a traditional trust, the Italian legal model at issue does not involve a transfer of ownership: the assets remain with the person entrusting them, while the trust company administers them in its own name. The case therefore required the ECJ to determine whether such an arrangement can nevertheless qualify as trust-like under Art. 31 of Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (hereafter referred to as the "Anti-Money Laundering (AML) Directive") and whether the rules governing access to the resulting beneficial-ownership information are compatible with the rights guaranteed by Arts. 7, 8 and 47 of the EU Charter of Fundamental Rights.

The judges in Luxembourg found no grounds for calling the validity of Art. 31 into question. They held that the provision is sufficiently precise to satisfy the principle of legal certainty and that access to beneficial-ownership information limited to persons demonstrating a legitimate interest is compatible with Arts. 7 and 8 of the Charter. They also ruled that Italian trust mandates may qualify as legal arrangements similar to trusts even when ownership of the assets is not transferred, as they can pose the same risk of concealing beneficial ownership and therefore necessitate the same level of transparency. Lastly, although decisions on exemptions from disclosure may be entrusted to an administrative authority, Art. 31(7a) of the AML Directive, read in the light of Art. 47 of the Charter, precludes national rules that do not allow the reviewing court to grant interim measures where an exemption is refused.

➤ *Background of the cases and questions referred*

Several Italian trust companies challenged, before the *Tribunale amministrativo regionale per il Lazio* (Regional Administrative Court, Lazio, Italy), national measures classifying their trust mandates as legal arrangements similar to trusts within the meaning of Art. 31 of the AML Directive. As a result of this classification, the companies are required to report information on the beneficial owners concerned

for inclusion in a special section of the Italian business register. Once registered, this information can be accessed by third parties demonstrating a legitimate interest upon application to the competent chamber of commerce. The chamber of commerce also decides on applications by beneficial owners for an exemption from disclosure. Although its decisions are subject to judicial review, the reviewing court is unable to grant interim relief where an exemption was refused.

Following the dismissal of their actions, the companies appealed to the *Consiglio di Stato* (Council of State, Italy), which referred several questions to the ECJ. In essence, the Council of Sate asked the ECJ:

- Is Art. 31 of the AML Directive, which regulates the beneficial ownership transparency, tracking, and registration requirements for trusts and similar legal arrangements, sufficiently precise to satisfy the principle of legal certainty and do the rules governing access to beneficial-ownership information comply with the rights to respect for private life and to the protection of personal data under Arts. 7 and 8 of the Charter?
- Can the concept of "other types of legal arrangements having a structure or functions similar to trusts" in Art. 31 of the Directive encompass arrangements under which ownership of the assets is not transferred to the person entrusted with their administration?
- Does Art. 31(7a) of the Directive, read in the light of Art. 47 of the Charter, permit an administrative authority to decide on exemptions from disclosure where the reviewing court is unable to grant interim relief?

➤ *The ECJ's reasoning on the validity of Art. 31 of the AML Directive*

The ECJ first examined whether the reference in Art. 31(1), (2) and (10) of the AML Directive to "other types of legal arrangements having a structure or functions similar to trusts" is sufficiently precise to satisfy the principle of legal certainty. It recalled that this principle does not prevent the EU legislature from using abstract legal concepts or leaving national authorities with some discretion, provided that the scope and exercise of this discretion are defined with sufficient clarity to enable the persons concerned to ascertain the extent of their obligations and regulate their conduct accordingly.

The Court found that these requirements are satisfied. Given the diversity of legal arrangements recognised under the laws of the Member States, the EU legislature was entitled to adopt a functional concept capable of encompassing different national models, rather than attempting to provide an exhaustive list.

Moreover, Art. 31(10), read in the light of Recital 29 of Directive 2018/843, requires Member States to notify the Commission of the types and defining features of legal arrangements they consider similar to trusts. The Commission is, in turn, required to publish this information in a consolidated list. According to the Court, this mechanism provides sufficient clarity as to which national arrangements fall within the scope of Art. 31 and enables the persons concerned to identify the obligations applicable to them. Therefore, the ECJ concluded that there are no grounds to call into question the validity of Art. 31(1), (2) and (10) in the light of the principle of legal certainty.

Second, the ECJ examined the compatibility of Art. 31(4), first subparagraph, point (c) of the AML Directive with the rights to respect for private life and the protection of personal data guaranteed by Arts. 7 and 8 of the Charter, insofar as it requires Member States to make information identifying the beneficial owners of such legal arrangements available to third parties.

While the Court acknowledged that this interferes with these fundamental rights, it found that the interference is justified. This is because the measure pursues the legitimate objective of preventing money laundering and terrorist financing by enhancing transparency regarding the natural persons who ultimately own or control assets. Such transparency helps create an environment that is less susceptible to misuse for illicit purposes. Extending access beyond competent authorities and obliged entities must be considered justified, as scrutiny by third parties with a legitimate interest provides an additional layer of oversight and can contribute to the detection and prevention of suspicious arrangements.

The ECJ also determined that the interference does not exceed what is strictly necessary to achieve this objective. Unlike the regime examined in *Luxembourg Business Registers* (→*eucrim 4/2022, 244–245*), Art. 31 does not grant unrestricted access to a potentially unlimited number of persons. Rather, access is limited to persons who can demonstrate a legitimate interest in the prevention or combating of money laundering, terrorist financing or the associated predicate offences. Moreover, Art. 31(7a) permits access to be restricted in exceptional circumstances where disclosure would expose the beneficial owner to serious and disproportionate risks.

➤ *The ECJ's reasoning on the scope of Art. 31*

Turning to the scope of Art. 31, the ECJ held that Italian trust mandates may qualify as "other types of legal arrangements having a structure or functions similar to trusts" by arguing that:

The wording of the provision calls for a broad interpretation capable of accommodating the diversity of trust-like arrangements recognised across the Member States. Accordingly, a legal arrangement need not replicate every characteristic of a traditional trust in order to fall within the scope of Art. 31. Since the features of such arrangements vary significantly between Member States and are shaped by their respective legal systems, the transfer of ownership cannot be re-

garded as an indispensable structural requirement.

The objective of Art. 31 is to ensure the effective prevention of money laundering by enhancing transparency with regard to trust-like legal arrangements and preventing the concealment of beneficial ownership. From this perspective, the formal transfer of ownership is not decisive. Even when the assets remain legally owned by the person entrusting them, such arrangements can pose the same risk of concealing the identity of the beneficial owner. Excluding them from the scope of Art. 31 would therefore jeopardise the effectiveness of the transparency regime established by this provision.

➤ *The ECJ's reasoning on exemptions and judicial protection*

Lastly, the ECJ examined whether decisions concerning exemptions from access to beneficial-ownership information can be entrusted to an administrative authority. According to the Court, Art. 31(7a) of the AML Directive does not, in principle, require such decisions to be taken by a court, and therefore permits the Italian system, under which the competent chambers of commerce determine whether an exemption from disclosure should be granted.

However, entrusting the initial decision to an administrative authority does not relieve Member States of their obligation to ensure effective judicial protection under Art. 47 of the Charter. The administrative decision must therefore remain subject to review by a court empowered, where necessary, to grant interim measures in order to preserve the full effectiveness of its final decision.

Although the Italian rules provide for judicial review of decisions taken by the chambers of commerce, they do not allow the reviewing court to grant interim protection where an exemption was refused. Art. 31(7a), read in the light of Art. 47 of the Charter, therefore precludes the Italian rules to that extent.

➤ *Put in focus*

The judgment further clarifies the limits established in the *Luxembourg Business Registers* case (see above). While unrestricted public access to beneficial-ownership information disproportionately interferes with the rights to privacy and data protection, access based on a demonstrated legitimate interest can strike an appropriate balance between these fundamental rights and the objective of effectively preventing money laundering. At the same time, the ECJ takes a functional approach to trust-like arrangements: their inclusion within the transparency regime depends on their structure, effects and potential to conceal beneficial ownership, rather than on their formal classification or the transfer of ownership. However, broad transparency obligations must be accompanied by effective procedural safeguards: where an exemption from disclosure is refused, judicial protection must include the possibility of granting interim measures. (JK)

Takedown of Major Cryptocurrency Laundering Service "AudiA6"

In June 2026, Europol reported that a major cryptocurrency laundering service known as „AudiA6" was dismantled in an international law enforcement operation. The service was used by ransomware groups and cybercriminal networks to launder stolen digital assets while obscuring financial trails. It is suspected of having laundered over €336 million from 2022 to 2025. The individuals behind „AudiA6" are also believed to have administered the dark web forum „Dark2Web", a marketplace used to advertise illicit services and facilitate contact between criminal actors.

Clients of „AudiA6" transferred cryptocurrency to wallets controlled by the group and received „cleaned" funds within approximately one hour through layered transactions designed to obscure the origin of the funds, while commissions were requested ranging between three and ten percent.

On 10 June 2026, a coordinated action resulted in the arrest of two alleged administrators, the search of three properties, the takedown of 25 domains, as well as the seizure of more than 30 servers, over 80 vehicles, multiple properties, and over €86,000. Law enforcement freezed €692,000 in cryptocurrency. The clear web and dark web sites of „AudiA6" and „Dark2Web" were replaced with seizure banners. More than 6000 Know Your Customer (KYC) records linked to mule accounts were identified. In addition, the investigators identified a number of further domains that will be subject to blocking measures.

The case reflects an emerging trend identified in Europol assessments: the rise of industrial-scale cryptocurrency laundering services powering the cybercrime economy. Ransomware groups increasingly rely on chain-hopping, decentralised exchanges, and mixer-type services to obscure transaction flows and rapidly move illicit funds. The use of fraudulent exchange accounts, mule wallets, and privacy-enhancing tools continues to complicate anti-money laundering efforts, contributing to the integration of laundering services into the cybercrime supply chain.

To delve deeper into these evolving threats, Europol is organising a series of webinars dedicated to cybercrime trends. Further details and registration information can be found here. (CR)

Environmental Crime

Environmental Crime Directive: Eurojust Note on Judicial Cooperation

spot light

The new Environmental Crime Directive was to be transposed into national law by EU Member States by 21 May 2026. The Directive establishes minimum EU-wide standards for the definition of environ-

mental criminal offences and penalties, replacing the previous 2008 legislation. In addition, it introduces a significantly strengthened legal framework for preventing, detecting, investigating, prosecuting, and adjudicating environmental offences across the EU (→eucrim 1/2024, 32–33).

To support practitioners in the application of the new EU rules, Eurojust published a note on 29 May 2026 providing a concise overview of the Directive. The note focuses on provisions with direct implications for international judicial cooperation in criminal proceedings involving environmental offences. It also highlights the assistance that Eurojust can provide to practitioners in cross-border environmental crime investigations in light of the Directive's novelties. In this context, the note outlines the Directive's key provisions, in particular those relating to the definition of offences, penalties, jurisdiction, and cross-border cooperation. Eurojust's key statements on the Directive are as follows:

- **Definition of offences:** The Directive broadens the range of conduct classified as criminal, removing Member States' ability to opt for administrative sanctions in relation to such conduct. It significantly enhances the harmonisation of definitions of environmental criminal offences across the EU, thereby strengthening legal certainty and ensuring compliance with the principle of legality. Compared to the 2008 Environmental Crime Directive, six new types of criminalised conduct have been introduced, while most existing offences are now subject to an expanded scope and lower criminal liability thresholds. In total, 20 environmental criminal offences have been established.
- **Penalties:** The Directive introduces stricter criminal penalties by specifying the types and levels of sanctions applicable to both natural and legal persons. This development facilitates meeting the crime severity threshold required for cross-border judicial cooperation, thereby supporting the use of international cooperation instruments and specialised investigative tools.
- **Jurisdiction and conflicts of jurisdiction:** The Directive lays down jurisdictional rules for environmental criminal offences, defining when Member States are obliged to establish jurisdiction and when they may exercise extraterritorial jurisdiction. Where an offence falls within the jurisdiction of more than one Member State, the Directive requires the Member States concerned to cooperate in order to determine the most appropriate forum for prosecution. Where appropriate, Member States must refer conflicts of jurisdiction in criminal proceedings to Eurojust.
- **National coordination:** Member States are required to establish mechanisms for strategic and operational coordination among all competent national authorities involved in combating environmental crime.
- **EU-level cooperation:** The Directive explicitly reinforces the role of Eurojust in providing technical and operational support to national authorities, thereby facilitating coordination in cross-border environmental crime investigations.

Eurojust concluded that the provisions of the Directive are expected to have direct positive implications for the cross-border cooperation at the judicial level. However, the Agency also stressed that environmental crime investigations are usually complex and resource-intensive, and require a multidisciplinary approach combining means of both administrative and criminal law, and highly specialised legal, technical and scientific knowledge. In this context, Eurojust highlighted the importance of cooperation among national authorities, as well as with international organisations and experts, to ensure effective and efficient investigations and prosecutions. (CR)

Cybercrime

IOCTA 2026

spot light

On 28 April 2026, Europol published the 11th edition of its 2026 Internet Organised Crime Threat Assessment (IOCTA).

Under the title "The evolving threat landscape: how encryption, proxies and artificial intelligence are expanding cybercrime", the assessment provides a detailed analysis of significant developments, changes, and emerging threats in cybercrime in 2025. The report contains four chapters looking at cybercrime enablers, the criminal infrastructure behind online fraud schemes, cyber-attacks, and online child sexual exploitation.

Regarding cybercrime enablers, the report highlights how cybercriminals are adopting more resilient, anonymous, and sophisticated methods to evade detection and maintain their operations despite law enforcement efforts. Key developments include:

- Dark web marketplaces are increasingly fragmented, with many platforms specializing in specific criminal activities rather than offering a broad range of illicit services;
- Criminal marketplaces remain highly resilient, as new platforms quickly emerge and online forums enable the migration of users and vendors after disruptions;
- Cryptocurrencies remain the preferred payment method for ransomware attacks;
- The growing use of privacy-focused digital currencies and transaction-mixing services makes financial investigations more difficult;
- The distinction between the surface web and the dark web is becoming less clear as encrypted communication platforms and anonymous services increasingly connect both environments;
- Criminals exploit weaknesses in the domain name registration process by using newly registered domains before

law enforcement agencies can detect and disrupt them;

- Cybercriminals are deploying increasingly complex technical infrastructures, including multilayered hosting arrangements, anonymous routing techniques, and residential proxy networks.

In the area of criminal infrastructure behind online fraud schemes, the report warns that online fraud is becoming more sophisticated, scalable, and difficult to detect, driven by evolving criminal infrastructures and the growing use of advanced technologies:

- Online fraud schemes continue to expand;
- Phishing remains one of the most common fraud methods;
- The misuse of subscriber identity module box devices enables criminals to conduct large-scale attacks through mass communication and identity spoofing;
- Some criminal groups are moving away from commercial hosting providers and building their own infrastructure to avoid identity verification requirements;
- The theft of digital assets has evolved into a crime-as-a-service model;
- Generative artificial intelligence is helping fraudsters create more convincing and personalized scams;
- Autonomous artificial intelligence systems are expected to automate parts of the criminal process and significantly increase the scale and effectiveness of online fraud.

Regarding cyber-attacks, the report highlights a ransomware ecosystem that is becoming more fragmented, competitive, and adaptable, with criminal groups continuously evolving their methods and services.

- The ransomware landscape remains highly volatile, with new ransomware brands emerging due to competition among criminal groups, law enforcement disruptions, and access to new technologies;
- Ransomware attacks continue to increase, with more than 120 active ransomware brands observed during 2025;
- Ransomware-as-a-service groups are expanding their offerings to attract affiliates, including the integration of artificial intelligence tools and more customizable services;
- Significant overlaps exist between different ransomware operations, as affiliates and administrators often work across multiple brands and campaigns;
- Affiliates and administrators play a central role in sustaining and expanding the ransomware ecosystem, contributing to its resilience despite enforcement actions;
- Hybrid threat actors increasingly use cybercriminal networks as proxies to conduct distributed denial-of-service attacks, ransomware operations, data theft campaigns, and attacks against strategically important targets.

Lastly, the report highlights an increasingly complex and harmful landscape of online child sexual exploitation, driven by financial incentives, new technologies, and secure communication platforms:

- Extortion remains a major component of child sexual exploitation, with victims coerced into sending money, producing additional sexual material, or engaging in harmful and abusive acts under threat;
- The trade in child sexual abuse material for financial gain is increasing, alongside a persistent threat from live-distant child abuse and a growing number of scam platforms involved in selling or distributing such material;
- The emergence of artificially generated child sexual abuse material is creating additional challenges for detection, victim identification, and law enforcement investigations;
- End-to-end encrypted messaging applications are widely used by offenders for grooming, sharing illegal material, and coordinating activities due to the difficulty authorities face in accessing communications;
- Criminal networks are exploiting both financial incentives and technological tools to expand the scale, reach, and concealment of child sexual exploitation activities.

Looking ahead, the report warns of a future in which cybercrime becomes increasingly automated through advanced artificial intelligence systems capable of carrying out criminal activities with minimal human involvement. Cybercriminal groups are expected to become more resilient and harder to identify, while collaborations between state-linked actors and criminal networks may intensify cyber threats against governments, businesses, and critical infrastructure. Online fraud is likely to grow in scale and sophistication as artificial intelligence enables highly convincing scams and automates criminal operations. The spread of synthetic child sexual abuse material, combined with the wider use of end-to-end encryption and decentralized platforms, is expected to create significant challenges for law enforcement. Criminals are also likely to continue exploiting cryptocurrencies, offshore financial services, and fintech platforms to move and conceal illicit funds. (CR)

Europol Report Outlines Transition to Post-Quantum Cryptography for Financial Institutions

On 21 January 2026, Europol and its partners published a joint report entitled „Prioritising Post-Quantum Cryptography Migration Activities in Financial Services". The report offers financial institutions a structured, risk-based approach to preparing for the transition to post-quantum cryptography (PQC). This involves using encryption methods that are designed to remain secure even against attacks from quantum computers. As advances in quantum computing are expect-

ed to compromise the long-term security of current encryption standards, financial institutions should start preparing for these future risks by transitioning to more secure cryptographic methods. They should plan the shift to quantum-safe security, determining priorities based on system vulnerability (quantum risk) and the time required for upgrades (migration time). This information can then be used to prioritise actions and implement changes step by step.

According to the report, a critical first step is to identify all business use cases that rely on public key cryptography. This inventory enables the development of a prioritised transition roadmap, with the quantum risk of each use case being assessed based on three parameters:

- "Shelf life of protected data", which refers to how long the data remains sensitive;
- "Exposure", which indicates the extent to which data is accessible to potential attackers;
- "Severity", which reflects the business impact of a potential compromise.

When the quantum risk is assessed, organisations can prioritise actions based on the migration time of each use case, i.e., the complexity and timeline required to achieve quantum safety for a particular use case. The report explains how to assess risk using a Quantum Risk Score, set up a Migration Time Score, and determine migration priorities. It also provides example use cases to demonstrate the methodology and warns against cryptographic antipatterns in cybersecurity. These are commonly used but flawed practices that can increase vulnerabilities, operational risk, and long-term technical debt, particularly in financial institutions. Identifying and addressing them early on can strengthen security, improve cryptographic maturity, and support faster and more flexible migration to future-ready systems.

The report concludes that the transition to quantum-safe cryptography is not merely a technical upgrade. It is a strategic imperative that demands foresight, coordination, and disciplined execution across the entire ecosystem, and is necessary for businesses to position themselves as leaders in secure digital innovation for the quantum era. (CR)

Operation "Alice" Exposes Fraudulent CSAM Platform

On 9 March 2026, a global operation led by German law enforcement authorities and supported by Europol targeted a major dark web network known as „Alice with Violence CP". Taking place from 9 to 19 March across 23 countries, the operation initially focused on the platform operator but ultimately resulted in the identification of hundreds of customers, prompting further investigations.

Over the last five years, investigators discovered that one individual had operated over 373,000 onion domains on the dark web. Over 90,000 of these domains advertised child sexual abuse material (CSAM), offering paid „packages" via email registration and Bitcoin payments, but the advertised content was never delivered. The sites also promoted other fraudulent „cybercrime-as-a-service" offerings with the same goal of obtaining payment without delivery.

The operation identified one main suspect, a 35-year-old man based in China, shut down over 373,000 websites, seized 105 servers, and identified 440 customers worldwide. (CR)

Organised Crime

Commission Unveils Maritime and Ports Strategies

On 4 March 2026, the European Commission adopted a new EU Industrial Maritime Strategy and an EU Ports Strategy aimed at strengthening competitiveness, sustainability, and security across the maritime sector.

The Industrial Maritime Strategy focuses on reinforcing Europe's global leadership in shipbuilding and shipping through investment in innovation, digitalisation, and decarbonisation.

The Ports Strategy addresses the role of ports as critical infrastructure for trade, energy, and security. It sets up a comprehensive framework to step up the competitiveness, resilience, security and sustainability of Europe's ports. Among the five priorities figures also the support for protecting and securing EU ports. In this context, the Commission proposes measures against organised crime and cybersecurity risks. New initiatives will include:

- Establish frameworks for third-country port risk assessments and for background checks for port workers;
- Update and revise guidance on emerging threats;
- Improve alignment of customs controls across ports in the European Union together with better security protocols worldwide;
- Establish a new forum designed to facilitate the exchange of best practices among Member States' cybersecurity and port authorities.
- Carry out an EU-wide security risk assessment to identify the most pressing cybersecurity risks and measures to mitigate them.

Together, the strategies aim to modernise the sector, support the green transition, and reinforce the EU's economic security, with implementation overseen by a new high-level Maritime Industries and Ports Board. The measures with regard to security build on the European Ports Alliance private-public partnership – an initiative that was launched in January 2024 to strengthen cooperation between European ports in the fight against organised crime and drug trafficking (→eucrim 1/2024, 30). (AP)

Europol Report Highlights Shift in Maritime Cocaine Trafficking

On 27 January 2026, Europol published a report entitled „Diversification in Maritime Cocaine Trafficking Modi Operandi". The report analyses the evolving tactics used by criminal networks to traffic cocaine into Europe via maritime routes.

Setting the scene: The expansion of coca cultivation and increased efficiency in Latin America have led to high levels of cocaine production. Combined with rising cocaine use in several EU Member States, both supply and demand remain high, sustaining a lucrative market that encourages criminal networks to develop more sophisticated trafficking methods. While ports such as Antwerp, Hamburg, and Rotterdam have traditionally been key entry points for large-scale maritime cocaine trafficking into Europe, targeted law enforcement actions and the launch of the European Ports Alliance Public Private Partnership (→eucrim 1/2024, 30) have led to a decrease in cocaine seizures in these ports, having prompted criminal networks to adapt their transportation methods, concealment techniques, and routes.

According to Europol's report, new modi operandi include:

- Diversifying routes and methods by bypassing major ports through at-sea drop-offs, transfers, semi-submersibles, and non-commercial vessels, making detection more difficult;
- More sophisticated concealment techniques, hiding cocaine in industrial equipment, machinery, and materials such as food, plastics, and textiles, which complicates detection using scanners, sniffer dogs, and forensic tests;
- Technological advancements, including encrypted communication, autonomous vessels, and drones, to enhance operations and evade detection.

Against this backdrop, the report concludes that addressing these challenges requires a coordinated, intelligence-led approach integrating maritime, financial, and technological capabilities. Monitoring should extend beyond commercial ports to smaller harbours, coastal areas, and open-sea routes. Financial investigations must adapt to fragmented transactions and informal maritime economies. Forensic and technical expertise should be applied earlier to detect hidden compartments, chemically concealed drugs, and extraction laboratories. Lastly, cooperation among law enforcement, customs, port authorities, and the private sector remains essential to securing supply chains and sharing data in real time, supported by cross-border investigations, integrated analysis platforms, and common risk indicators.

Europol will support the fight against the threat of cocaine trafficking through its dedicated Drugs Unit. The Agency will also provide analyses and coordinate EU-wide operations as well as deploy experts on the ground. (CR)

Project A.S.S.E.T. – New Benchmark for International Cooperation in Global Asset Seizure

From 19–22 May 2026, Europol conducted the third and most successful operational week of Project A.S.S.E.T. (Asset Search & Seize Enforcement Taskforce). Project A.S.S.E.T., organised by Europol's European Financial and Economic Crime Centre (EFECC), supports the fight against serious and organised crime and the seizure of criminal assets.

The operation was carried out in close cooperation with a broad international network of partners, including law enforcement agencies from 31 countries worldwide, asset recovery offices (AROs), financial intelligence units (FIUs), specialised anti–money laundering and organised crime units, as well as leading private-sector partners from the financial services and cryptocurrency sectors.

Project A.S.S.E.T. was further supported by Eurojust, INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC), the EPPO, and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), highlighting the unprecedented level of cooperation.

As a result of this coordinated cooperation, authorities identified and traced 884 bank accounts, 80 companies, 55 crypto wallets, 74 vehicles and one vessel, and 44 real estate properties, including six valued at a combined €5.64 million. They also located two suspected criminals, with one arrest carried out via the European Network of Fugitive Active Search Teams (ENFAST).

Furthermore, the operation generated significant intelligence on criminal financial networks and emerging ML methods, supporting ongoing investigations across participating jurisdictions and strengthening future cross-border enforcement efforts. (CR)

Terrorism

Commission Presents New ProtectEU Counterterrorism Agenda

On 26 February 2026, the European Commission presented a new ProtectEU agenda to prevent and counter terrorism and violent extremism in the EU. The agenda aims to update the Union's response to an evolving threat landscape, including online radicalisation, the growing involvement of minors, the misuse of new technologies, and increasing links between terrorism, organised crime, and hostile foreign interference.

The Commission identifies six areas for action: (1) anticipating threats, (2) preventing radicalisation, (3) protecting people online, (4) securing public spaces and critical infrastructure, (5) improving responses to attacks, and (6) strengthening cooperation with international partners.

Key measures include reinforcing EU-level intelligence analysis and Europol's analytical and open-source intelligence capacities, as well as expanding research on risks linked to artificial intelligence, crypto-assets, drones, and 3D-printed weapons. The agenda also introduces a prevention toolbox targeting the radicalisation of minors and a €5 million Community Engagement and Empowerment Programme focused on youth, digital resilience, and community cohesion.

In the online sphere, the Commission announces a possible revision of the Terrorist Content Online Regulation (→eucrim 2/2022, 112) following its 2026 evaluation and commits to stricter enforcement of the Digital Services Act. It also proposes upgrading the EU Crisis Protocol into a broader Online Crisis Response Framework to improve coordination between authorities and platforms.

Further measures address physical security, including improved information-sharing through the Schengen Information System, possible extensions of advance travel information rules, and additional investments in the protection of public spaces and critical infrastructure. The agenda also proposes new tools to track terrorist financing, including a future EU Financial Data Retrieval System, alongside revisions of Europol's and Eurojust's mandates.

The agenda builds on the broader ProtectEU, the European Internal Security Strategy presented in April 2025, which sets out a comprehensive framework for strengthening EU internal security and emphasises anticipatory action, cross-sectoral cooperation, and increased investment. Eucrim has previously reported on this strategy (→eucrim 1/2025, 3–4) and its subsequent assessment by the Council, noting both general support by Member States and an ongoing controversy surrounding access to data for law enforcement (→eucrim 2/2025, 110–111). (AP)

EU Expands Terrorist Sanctions to Leaders and Support Networks

On 26 February 2026, the Council strengthened the EU's counterterrorism sanctions regime by expanding the scope of the EU terrorist list and updating its legal framework.

The reform broadens the listing criteria, allowing the EU to explicitly target leading members of listed organisations as well as persons associated with them, including those involved in financing, training, or recruitment. This clarifies and extends the reach of the regime beyond direct perpetrators.

In addition, a travel ban has been introduced for listed individuals, complementing existing measures such as asset freezes and a prohibition on making funds or economic resources available. The change aligns the regime more closely with other EU sanctions frameworks, such as those directly targeting ISIL/Da'esh and Al-Qaida.

The update was formalised through Council Decision (CFSP) 2026/455 and Council Regulation (EU) 2026/456, which amend and partially replace elements of the earlier framework under Common Position 2001/931/CFSP and Regulation (EC) No. 2580/2001, modernising a regime originally established in the aftermath of the 09/11 attacks.

At the same time, the Council concluded its regular review of the EU terrorist list and maintained all existing listings unchanged. Individuals and entities on the list therefore remain subject to the same restrictive measures.

While the reform adjusts the scope and structure of the regime, its core elements – including asset freezes, funding prohibitions, and the definition of terrorist acts – remain unchanged. The changes instead focus on expanding who can be targeted within and in connection with listed organisations and on strengthening the overall effectiveness of the framework. (AP)

Europol Coordinates Largest Action against Audio-Based Terrorist Propaganda

In response to the growing presence of terrorist content on audio-sharing platforms, Europol coordinated the largest Referral Action Day to date at the beginning of March 2026, targeting propaganda used by groups across the ideological spectrum, including jihadist and violent right-wing extremist networks.

Audio propaganda is increasingly recognised as a powerful radicalisation tool. Unlike videos or images, it is harder to moderate, as identifying extremist messaging requires linguistic expertise and contextual understanding. As a result, such content can circulate undetected and remain accessible to vulnerable individuals. While music and songs have long been used in terrorist propaganda to trigger emotional responses, evoke anger or grievance, glorify sacrifice and martyrdom, and reinforce group identity through "us versus them" narratives, they now also serve as a softer entry point into extremist ecosystems online. Compared with explicit ideological speeches, songs may appear cultural or inspirational, enabling extremist messaging to reach wider audiences.

The Referral Action Day was coordinated by Europol's EU Internet Referral Unit (EU IRU) and Hungary, bringing together investigators from 13 countries. It led to the referral of 17,298 URLs across 40 platforms, representing over 1,100 hours of terrorist and extremist propaganda. The content was referred to service providers for assessment under their terms of service, with 77% removed so far.

The EU IRU at Europol fights publicly available terrorist and violent extremist content online. It flags extremist propaganda to online platforms for voluntary removal. Additionally, the unit provides critical internet-based investigative support to EU Member States' law enforcement.(CR)

Procedural Law

Procedural Safeguards

ECJ Clarifies Limits of Appellate Reasoning under the Presumption of Innocence

On 30 April 2026, the ECJ delivered its judgment in Case C-748/24 (Kotaňák) concerning the presumption of innocence under Directive 2016/343. The case raised the question of how far an appellate criminal court may go, at a preliminary stage of proceedings, when assessing incriminating evidence, and whether its findings may bind the lower court if they appear to anticipate the accused person's guilt.

➤ *Background of the case*

The case concerned criminal proceedings in Slovakia against AC for defamation. The accused had allegedly posted several videos online containing false allegations about another person. The court of first instance twice discontinued the proceedings, finding that the conduct described in the indictment did not constitute a criminal offence.

The prosecutor appealed. The appellate court set aside the discontinuance orders and referred the case back to the lower court. In its reasoning, however, the appellate court used strong factual language, stating, among other things, that the evidence showed "beyond doubt" that the accused had used lies and that certain events described by him had never taken place.

The criminal court now competent to decide on the criminal proceedings against AC at first instance was concerned that the statements by the appellate court might breach the presumption of innocence. Under Slovak procedural law, the lower court would normally be bound by the legal views expressed by the appellate court. It therefore asked the ECJ whether such appellate findings were compatible with Directive 2016/343 on the presumption of innocence and what the lower court should do if they were not.

➤ *The ECJ's ruling*

The ECJ held that Directive 2016/343 does not prevent an appellate criminal court from examining incriminating evidence in detail at a preliminary stage of the proceedings. Nor does the Directive, as such, prevent the appellate court from assessing whether the constituent elements of the alleged offence may be present, even where the accused has not yet had the opportunity to comment on all evidence.

However, the ECJ stressed that the reasoning must not imply guilt before it is legally established. The key question is whether the decision's wording, context, and overall reasoning convey only suspicion or instead a premature finding of guilt. It noted that expressions suggesting that all elements of the offence are already established may indicate a breach of the presumption of innocence, but left the final assessment to the national court.

Looking at the binding effect of appellate court decisions under national law, the ECJ held that, if the lower court finds that the appellate court's rulings are incompatible with the presumption of innocence, it must disregard those rulings, even if national law would normally require it to follow them. This follows from the direct effect of Art. 3 of Directive 2016/343 and the primacy of EU law. However, the lower court need not disregard the appellate decision in its entirety: it may still have to comply with procedural measures ordered by the appellate court, such as continuing the proceedings following remittal. (AP)

ECJ: Victim Participation Not Required in Proceedings to Quash Convictions Rendered *in absentia*

On 23 April 2026, the ECJ delivered its judgment in Case C-24/26 PPU, Casotta. In the first place, the ECJ clarified the scope of victims' rights under Directive 2012/29/EU in proceedings seeking to reopen criminal cases concluded by a final conviction rendered in the defendant's absence. It held that the Victims' Rights Directive does not require Member States to inform victims who did not join the criminal proceedings as civil parties of an application to quash such a conviction. Nor does it oblige them to grant these victims the right to participate in the ensuing proceedings. In the second place, the ECJ confirmed that Directive (EU) 2016/343 does not preclude Member States from granting persons convicted in absentia access to a new trial under more favourable conditions than those required by EU law.

➤ *Background of the case and questions referred*

The request for a preliminary ruling was made by the *Corte d'appello di Roma* (Court of Appeal, Rome, Italy). Under Art. 629-bis of the Italian Code of Criminal Procedure, a person convicted *in absentia* may apply to have a final conviction quashed and the criminal proceedings reopened if the conditions for conducting the trial in his or her absence were not fulfilled. If the application is granted, the conviction is set aside and the proceedings resume.

The referring court raised two questions:

- Do Arts. 6, 10 and 18 of Directive 2012/29 preclude national legislation under which a victim who has not joined the criminal proceedings as a civil party is neither informed of an application to reopen the proceedings nor entitled to participate in them?
- Do Arts. 8 and 9 of Directive 2016/343, read in the light of the prohibition of abuse of rights under Art. 54 CFR, preclude national case law on the reopening of convictions rendered *in absentia* given that the deliberate avoidance of becoming aware of the criminal proceedings may be estab-

lished only by direct proof? In the referring court's view, this evidentiary standard results, in practice, in an almost systematic reopening of proceedings and may reward evasive conduct by defendants.

➤ *The ECJ's ruling on the interpretation of the Victims' Rights Directive*

As regards the first question, the Court observed that information concerning an application to reopen criminal proceedings falls, if at all, within the scope of Art. 6(2)(b) of Directive 2012/29, which concerns the victim's right to receive information on the „state of the criminal proceedings." However, the extent of that information right depends on the victim's procedural role under national law. Accordingly, where national law grants the relevant procedural rights only to victims who have joined the proceedings as civil parties, the Directive does not require Member States to notify victims who have not acquired that status. The Court added that this interpretation does not leave victims without protection. Art. 6(5) and (6) of the Directive require Member States to inform victims of the offender's release or escape, irrespective of their participation as civil parties in the original proceedings.

The Court reached the same conclusion with regard to the right to be heard under Art. 10 of the Directive. While this provision guarantees victims the opportunity to be heard during criminal proceedings, it does not confer a right to be heard at every stage of those proceedings. Its purpose is to enable victims to participate in proceedings concerning the offence committed against them, notably by contributing to the establishment of the relevant facts and the gathering of evidence on the alleged offence and the harm suffered. By contrast, the purpose of proceedings to reopen a final conviction rendered *in absentia* is to determining whether the procedural conditions for conducting the original trial in the defendant's absence were met, particularly whether the defendant deliberately avoided becoming aware of the proceedings. Since neither the defendant's criminal liability nor the merits of the conviction or sentence are at issue, the rationale underlying Art. 10 does not require the victim to be heard again.

Nor does Art. 18 of the Directive alter this conclusion. The Court observed that this provision concerns the protection of victims against secondary and repeat victimisation during criminal proceedings. It governs *how* victims are to be protected during questioning, but not *whether* they may be questioned again in subsequent proceedings at all. Accordingly, Art. 18 cannot be interpreted as conferring a right to participate in proceedings to reopen a final conviction solely in order to prevent a new trial and the possibility of renewed questioning.

➤ *The ECJ's ruling on the interpretation of the Presumption of Innocence Directive*

Turning to the second question, the Court recalled that, under Arts. 8(2) and 9 of Directive 2016/343, as interpreted in its settled case law (most recently in Case C-135/25 PPU, *Kachev*), a person convicted *in absentia* may be refused a new trial if he or she deliberately avoided becoming aware of the criminal proceedings. The Directive does not require direct proof of such conduct; it may also be established on the basis of precise and objective indicia. Although the referring court considered such indicia to be present in the case before it, the Court held that EU law does not preclude Member States from applying a stricter evidentiary standard. Referring to recital 48 of the Directive, it observed that the Directive lays down minimum rules only and therefore allows Member States to provide a higher level of protection. Accordingly, Member States remain free to require direct proof that the person deliberately avoided becoming aware of the proceedings before refusing to reopen them.

Finally, the Court rejected the referring court's argument that an application to reopen the proceedings under the national rules at issue could constitute an abuse of rights within the meaning of Art. 54 CFR. It held that, where a person convicted *in absentia* seeks a new trial on the basis of safeguards exceeding the minimum standards laid down in Directive 2016/343, the right relied on is conferred by national rather than EU law. Exercising that right therefore cannot amount to an abuse of rights under EU law.

➤ *Put in focus*

Notably, the judgment illustrates the different implications of the minimum-harmonisation approach underlying both directives. While Member States remain free to grant persons convicted *in absentia* procedural safeguards exceeding the minimum standards set out in Directive 2016/343, Directive 2012/29 does not require them to afford victims procedural rights that go beyond those attached to their status under national law. The information and participation rights at issue therefore depend on the victim first acquiring a specific procedural status, such as that of a civil party. (JK)

AG: Questioning Without a Lawyer after Deadline for Appearing Has Passed Contravenes EU Law

In two parallel infringement proceedings – *Commission v Hungary* C-660/24 and *Commission v Czech Republic C-681/24* – Advocate General (AG) *Tamara Ćapeta* concluded on 12 March 2026 that Hungary and the Czech Republic have failed to correctly transpose key provisions of Directive 2013/48/EU on the right of access to a lawyer in criminal proceedings.

The cases concern national legislation permitting authorities to question suspects without the presence of

a lawyer if no lawyer appears within a specified time limit (two hours in Hungary; up to 48 hours in the Czech Republic). According to the European Commission, such rules undermine the Directive's guarantee that suspects must be able to exercise their rights of defence "practically and effectively," including during police questioning.

➤ *A Fundamental disagreement on the scope of the right*

At the core of both cases lies a disagreement over how the right of access to a lawyer under Art. 3 of the Directive should be understood.

The Commission argued that the Directive establishes a general rule requiring the presence of a lawyer during questioning, subject only to narrowly defined exceptions. By contrast, Hungary and the Czech Republic maintained that the Directive merely requires that suspects be given the opportunity to access a lawyer, not that questioning must be delayed until a lawyer is actually present.

Ms *Ćapeta* clearly endorsed the Commission's interpretation. She held that Art. 3(3)(b) of the Directive, which provides for the right of suspects to have their lawyer "present and participate effectively when questioned," must be understood as requiring the actual (physical) presence of a lawyer during questioning as a rule.

➤ *Strict limits on derogations*

Ms *Ćapeta* emphasised that questioning without a lawyer constitutes a derogation from that general rule. Such derogations are permissible only under the strict conditions set out in Art. 3(6) of the Directive, which allows temporary departures in exceptional circumstances and on the basis of compelling reasons, such as preventing serious harm or substantial jeopardy to criminal proceedings.

In her view, the national provisions at issue do not meet those requirements. They establish a general and automatic mechanism allowing questioning in the absence of a lawyer once a certain time has elapsed, without any case-specific assessment or demonstration of urgency. As such, they exceed the exhaustive system of derogations provided for in the Directive.

Ms *Ćapeta* further clarified that the Directive does not leave Member States discretion regarding the presence of a lawyer. The reference to national law in Art. 3(3)(b) concerns only the modalities of participation, not the existence of the right itself.

➤ *Effectiveness of defence rights*

A central element of Ms *Ćapeta*'s reasoning is the requirement that defence rights must be guaranteed in a practical and effective manner. Allowing questioning to proceed simply because a lawyer has not appeared within a fixed time period risks undermining that requirement, particularly at the pre-trial stage, where suspects are most vulnerable.

She rejected arguments that such rules are necessary to prevent abuse or delays in criminal proceedings and noted that national authorities have alternative means at their disposal, such as appointing substitute counsel, to ensure both the effectiveness of investigations and the protection of defence rights.

➤ *Relationship with ECHR standards*

Both Member States relied on case law of the European Court of Human Rights (ECtHR) to argue that the Directive does not require the physical presence of a lawyer in all cases. Ms *Ćapeta* acknowledged that the European Convention on Human Rights (ECHR) sets a minimum standard of protection, but stressed that EU law may provide more extensive safeguards.

In any event, she considered that Strasbourg case law itself highlights the importance of a lawyer's presence during police questioning as a key safeguard against coercion and as a means of ensuring the effective exercise of defence rights.

➤ *Additional breach by Hungary: Waiver of rights*

In the case against Hungary, Ms *Ćapeta* also found a failure to transpose Art. 9 of the Directive on the waiver of the right of access to a lawyer.

Although Hungarian law characterises this right as inalienable, suspects may in practice choose not to exercise it. Ms *Ćapeta* held that such situations are functionally equivalent to a waiver and therefore require the safeguards laid down in Art. 9, including that the decision be informed, voluntary, unequivocal, and properly recorded, and that it be revocable.

The absence of specific provisions implementing those safeguards was found to constitute a further infringement.

➤ *Implications for the EU's Area of Freedom, Security and Justice*

The Opinions underline the central role of the right of access to a lawyer as a cornerstone of fair trial rights within the EU's Area of Freedom, Security and Justice. By interpreting the Directive as requiring the presence of a lawyer during questioning as a rule, Ms *Ćapeta* adopts a reading that strengthens procedural safeguards and reinforces mutual trust between Member States' criminal justice systems. (AP)

Data Protection

ECJ Clarifies Limits on Police Collection of Suspects' Biometrics

spot light

On 19 March 2026, the ECJ delivered its judgment in Case C-371/24 *(Comdribus)* concerning the collection of biometric data by police authorities under Directive 2016/680. The case addressed whether police may systematically collect fingerprints and photographs from persons suspected of criminal offences, whether such collection must be individually justified, and whether refusal to cooperate may itself be punished as a separate offence.

➤ *Background of the case*

The case arose from criminal proceedings in France against a climate activist who had participated in an unauthorised demonstration in Paris. During police custody, he disclosed his identity but refused to be fingerprinted and photographed. He also refused to unlock his mobile phone. He was subsequently acquitted of the offences relating to the organisation of a demonstration and the refusal to provide access to his phone.

However, he was convicted of a fine of €300 for refusing to consent to the gathering of identification data, including fingerprints and photographs. This is a separate offence under French law. Court of Appeal in Paris asked the ECJ whether Directive 2016/680 precludes national legislation allowing the systematic collection of biometric data from persons reasonably suspected of having committed or attempted to commit an offence, and whether such refusal may be punished even if the person is not ultimately prosecuted or convicted for the underlying offence.

➤ *The ECJ's ruling*

The judges in Luxembourg held that fingerprints and photographs used for unique identification constitute biometric data and therefore fall within the special protection regime of Art. 10 of Directive 2016/680. Their collection is allowed only where it is strictly necessary, subject to appropriate safeguards, and authorised by EU or national law.

They further found that national legislation is contrary to Art. 10 of Directive 2016/680 if it provides for the systematic collection of biometric data from every person reasonably suspected of having committed or attempted to commit a criminal offence. The fact that a person is reasonably suspected is not, in itself, enough to establish that the collection of biometric data is strictly necessary. The competent authority must assess the necessity of the collection in each individual case, taking into account factors such as the nature and seriousness of the suspected offence, the circumstances of the case, possible links with other proceedings, and the person's criminal record or individual profile.

The ECJ also held that the competent authority must provide sufficient reasons, in each individual case, explaining why the collection of biometric data is strictly necessary. *Ex post* judicial review after the fact cannot substitute for this obligation: reasons must be provided so the data subject can effectively challenge the measure and the national court can assess its lawfulness.

Lastly, the ECJ ruled that EU law does not, in principle, preclude national legislation that criminalises refusal to submit to biometric data collection, even if the person is not ultimately prosecuted or convicted for the underlying offence. However, such a penalty is lawful only if the intended collection satisfies the strict necessity requirement in Art. 10 of Directive 2016/680 and the penalty imposed is proportionate as required by Art. 49(3) of the EU Charter of Fundamental Rights.

➤ *Put in focus*

The ECJ ruling in *Comdribus* imposes strict limits on the practice of police authorities routinely subjecting criminal suspects to identification procedures. In their response to the question referred from the Paris court, the judges in Luxembourg emphasise the importance of citizens' privacy: as biometric data falls within the category of particularly sensitive personal data, it enjoys enhanced protection. Accordingly, the processing of such data is only permissible if it is absolutely necessary and is accompanied by appropriate safeguards for the fundamental rights of the individuals concerned. The ruling is likely to have implications beyond France. It puts a stop to the practice of taking biometric data following every arrest, which is standard procedure in many countries. (AP)

CJEU Opens Door to Direct Challenges against EDPB Decisions

The ECJ has clarified the legal status of binding decisions adopted under the GDPR's consistency mechanism, holding that decisions of the European Data Protection Board (EDPB) that resolve disputes between national supervisory authorities constitute acts open to challenge before the EU Courts. In its 10 February 2026 judgment in Case C-97/23 P (*WhatsApp Ireland v European Data Protection Board*), the Grand Chamber of the ECJ found that such decisions produce legal effects vis-à-vis third parties and may directly affect the position of the data controller concerned.

By recognising that these decisions are not merely internal steps but reviewable EU acts, the ECJ set aside the General Court, which declared WhatsApp's action inadmissible (Case T-709/21), and referred the case back for a decision on the merits.

➤ *Facts of the case*

The case arose from an investigation by the Irish Data Protection Commission into WhatsApp's compliance with transparency obligations under the GDPR, following complaints from users and non-users. Acting as lead supervisory authority for cross-border processing, the Irish authority initiated an inquiry into WhatsApp's data-sharing practices, including its exchanges with other entities within the Meta group.

After a draft decision was circulated to other supervisory authorities under the GDPR cooperation mechanism, several authorities raised objections. As no consensus could be reached, the dispute was referred to the EDPB under Art. 65 GDPR.

In July 2021, the EDPB adopted a binding decision requiring the Irish authority to revise its draft. The instructions included that additional GDPR infringements be found, that certain data (including data resulting from "lossy hashing") be classified as per-

sonal data, and that the level of administrative fines be increased.

In August 2021, the Irish authority adopted its final decision, incorporating the EDPB's findings. It imposed a reprimand, corrective measures, and fines totalling €225 million. While WhatsApp challenged that final decision before the Irish courts, it also brought an action for annulment before the General Court against the EDPB decision itself.

The General Court dismissed that action as inadmissible, considering the EDPB decision to be a preparatory act without independent legal effects and not directly concerning WhatsApp. WhatsApp appealed.

➤ *Judgment and reasoning*

In its opposing judgment favouring the admissibility of the action under Art. 263 TFEU, the ECJ first clarified that the EDPB's decision cannot be regarded as intermediate step as it definitively determines its position on the issues referred to it and is legally binding on the national supervisory authorities concerned.

Second, the ECJ found that the decision was of direct concern to WhatsApp. The EDPB's findings – such as the identification of additional infringements and the requirement to increase fines – directly affected WhatsApp's legal situation. The Irish supervisory authority was bound by those findings and had no discretion to depart from them in its final decision. The absence of direct enforceability against WhatsApp did not preclude a finding of direct concern.

As a result, the Court of Justice rejected the General Court's approach, which had focused on the intermediate nature of the EDPB decision and the availability of judicial remedies at national level. Therefore, the existence of parallel remedies (before national courts against the final decision and before EU courts against the EDPB decision) does not exclude direct concern.

➤ *Significance*

The judgment strengthens judicial review within the GDPR enforcement system. It confirms that binding decisions adopted by the EDPB under Art. 65 GDPR are not merely internal coordination tools but legally relevant acts that can be challenged directly before the EU Courts.

More broadly, the ruling clarifies the structure of the GDPR's "composite" enforcement mechanism. While national supervisory authorities formally adopt the final decision, the EDPB's binding determinations on key legal issues can independently affect the rights and obligations of controllers. Those determinations must therefore be open to direct judicial scrutiny at EU level. (AP)

EU and Brazil Mutually Recognise Data Protection Standards

On 26 and 27 January 2026, the European Commission and Brazil adopted corresponding adequacy decisions, respectively, allowing personal data to be transferred between Brazil and the EU for business, administrative and research purposes without additional safeguards. These decisions followed the launch of the EU adequacy procedure in September 2025 and the subsequent green light European Data Protection Board for the Commission's draft decision. The Board highlighted the close alignment of Brazil's data protection framework with the General Data Protection Regulation (GDPR).

Pursuant to Art. 45(3) GDPR, the Commission recognised that Brazil ensures a level of data protection essentially equivalent to that guaranteed within the EU. The decision builds on the substantial development of Brazil's data protection framework, particularly the adoption of the General Data Protection Law (*Lei Geral de Proteção de Dados*, LGPD) in 2018 and the subsequent establishment of an independent national data protection authority.

In a joint press statement, *Michael McGrath* (Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection), and *Waldemar Gonçalves Ortunho Júnior* (President of the Brazilian Data Protection Authority) emphasised the benefits of these decisions for citizens, businesses and public authorities. By enabling personal data to flow in both directions without the need for additional safeguards or prior authorisations, the new framework is expected to boost digital trade, reduce compliance costs and enhance legal certainty. The decisions thereby create the world's largest area of free and safe data flows, encompassing approximately 670 million consumers.

The mutual adequacy decisions also complement the EU-Mercosur Partnership Agreement and the Interim Trade Agreement, both of which were signed on 17 January 2026. While the agreements seek to deepen political and economic ties and facilitate cross-border trade, the adequacy decisions reinforce these efforts by removing data protection-related barriers to personal data transfers between the EU and Brazil.

Notably, from a criminal justice perspective, the Brazilian adequacy decision expressly excludes transfers carried out exclusively for public security and law enforcement purposes. Therefore, the mutual adequacy decisions do not provide a legal basis for the direct exchange of operational data between law enforcement authorities. Such cooperation is governed separately, in particular by the EU-Brazil agreement on cooperation with and through Europol. This agreement enables the exchange of personal and non-personal data for law enforcement purposes and was signed in March 2025 and formally concluded in September 2025 (→eucrim 1/2025, 15).

Both sides will continuously monitor developments in the other party's data protection framework and conduct an initial review within four years.

If either framework ceases to ensure an adequate level of protection, the corresponding adequacy decision may be suspended, amended or repealed. (JK)

Freezing of Assets / Confiscation

ECJ Clarifies Scope of and Fundamental Rights Refusal Ground in Confiscation Regulation

spot light

On 17 March 2026, the ECJ, sitting as the Grand Chamber, delivered its judgment in Case C-8/24 (*D. d.o.o. v Županijsko državno odvjetništvo u Zagrebu*) concerning the mutual recognition of confiscation orders under Regulation 2018/1805. The case clarified whether the Regulation applies to confiscation orders issued in criminal proceedings that ended in an acquittal, but in which the court nevertheless ordered confiscation of property considered to be the proceeds of another criminal offence. Furthermore, the ECJ ruled on the ground for non-recognition due to a manifest breach of fundamental rights. It is the first ECJ judgment that interprets the 2018 Regulation on the mutual recognition of freezing and confiscation orders (→eucrim 4/2018, 201–202).

➤ *Background of the case*

The case arose from Slovenian criminal proceedings concerning alleged abuse of position or power. The defendants were ultimately acquitted of that offence. However, the Slovenian criminal court found that certain shares owned by a Croatian company constituted the proceeds of other criminal offences, namely acting to the detriment of creditors and money laundering. Those offences had not led to an indictment against the persons allegedly involved.

On that basis, the Slovenian court ordered confiscation of the shares. The order was transmitted to Croatia for recognition and execution under Regulation 2018/1805. The owner of the shares challenged recognition of the order, arguing, among other things, that the Regulation should not apply because the underlying proceedings had ended in an acquittal against other defendants and the confiscation related to offences for which no indictment against him had been brought. He also argued that his fundamental rights had not been respected in the Slovenian proceedings.

➤ *The ECJ's ruling*

The ECJ held that Regulation 2018/1805 does apply to such a confiscation order. It emphasised that the Regulation covers confiscation orders issued following proceedings in relation to a criminal offence, including confiscation without a final conviction. It was therefore irrelevant that the criminal proceedings ended in an acquittal, that the confiscation concerned property considered to be the proceeds of different offences, and that no indictment had been brought against the persons allegedly involved in those offences.

Looking at the possible refusal of recognition and execution on fundamental rights grounds, the ECJ held that Art. 19(1)(h) of Regulation 2018/1805 allows refusal, in exceptional circumstances, where specific and objective evidence provides substantial grounds to believe that execution would entail a manifest breach of a relevant Charter right.

The judges in Luxembourg stressed that this is a strict and exceptional ground for refusal. The executing authority does not have to carry out the two-step test developed in the European Arrest Warrant case law, requiring a prior finding of systemic or generalised deficiencies in the issuing Member State. Instead, it must conduct an individual assessment of whether execution would entail a manifest breach of fundamental rights in the particular case.

In the case at hand, the executing authority could not refuse recognition and execution solely on the basis of alleged fundamentalrights violations in the issuing Member State where the person had been properly served, in a language they understood, with parts of the judgment sufficient to enable an appeal, but did not exhaust the remedies available there. However, if the executing authority has doubts about service or the protection of fundamental rights, it must consult the issuing authority before refusing recognition or execution, in accordance with Art. 19(2) of Regulation 2018/1805. (AP)

ECJ Clarifies Protection of Bona Fide Mortgage Creditors in Cross-Border Confiscation

On 29 January 2026, the ECJ delivered its judgment in Case C-562/24 (Munik) concerning the mutual recognition and execution of confiscation orders under Framework Decision 2006/783/JHA. The case clarified when the rights of a mortgage creditor may prevent the execution of a confiscation order issued in another Member State, in particular where the creditor claims to be a bona fide third party.

➤ *Background of the case*

The case arose from criminal proceedings in Italy concerning serious fraud, money laundering, and participation in a criminal organisation. An Italian court ordered the confiscation of immovable properties of the company involved in the fraud scheme that were located in Slovenia and considered to constitute the proceeds of the offences. The confiscation order was transmitted to the Slovenian authorities for recognition and execution in March 2019.

Before the recognition and execution proceedings in Slovenia, in October 2018 and February 2019, a Slovenian company had registered judgment mortgages over one of the properties in order to secure its claims against the convicted company. It argued that it was a bona fide third party and that execution of the Italian confiscation

order would prejudice its rights as a mortgage creditor. The Slovenian court, which has to decide on the execution of the Italian confiscation order, therefore asked the ECJ whether such a creditor could fall within the protection of Art. 8(2)(d) of Framework Decision 2006/783.

According to this provision, „[t]he competent judicial authority of the executing State […] may also refuse to recognise and execute the confiscation order if it is established that: the rights of any interested party, including bona fide third parties, under the law of the executing State make it impossible to execute the confiscation order, including where this is a consequence of the application of legal remedies in accordance with Article 9".

➤ *The ECJ's ruling*

The ECJ held that a mortgage creditor may qualify as an interested party and, potentially, as a bona fide third party within the meaning of Art. 8(2)(d) of Framework Decision 2006/783. As a result, the competent authority of the executing Member State may refuse to recognise or execute a confiscation order if the creditor's rights make execution impossible under national law.

The ECJ clarified that, for the bona fide status, it must be established that that third party was not aware of the fact that the purpose of that transfer or acquisition was, for the suspected or accused person, to avoid confiscation. The creditor's bona fide status must be assessed by the national court in light of all the circumstances. The fact that the judgment mortgage was registered before the recognition and execution proceedings – and even before the confiscation order itself – may indicate the absence of fraudulent behaviour. At the same time, the national court must consider circumstances that may point in the opposite direction, such as whether insolvency or criminal proceedings were already pending when the mortgage was registered.

The ECJ therefore concluded that Art. 8(2)(d), read in light of Art. 17(1) of the Charter, allows the executing Member State to refuse recognition or execution of a confiscation order concerning immovable property that constitutes proceeds of crime where the rights of a bona fide mortgage creditor would make execution impossible. It remains for the national court to determine whether the creditor was in fact acting in good faith. (AP)

Cooperation

Police Cooperation

ECBA: Recommendations for Reform of INTERPOL's Systems

In February 2026, the European Criminal Bar Association (ECBA) released a report that made several proposals for improvements of operation of INTERPOL's data processing and oversight mechanisms. A particular focus is laid on the Commission for the Control of INTERPOL's Files (CCF). The report drew on ECBA members' practical experience of acting for individuals affected by INTERPOL alerts. It highlighted progress made following reforms of INTERPOL in the past decade as well as the need for further improvements. It identified ongoing challenges in relation to a range of topical areas:

- Delays;
- Pre-emptive requests;
- Wanted person diffusion notices;
- The recognition of extradition decisions;
- INTERPOL's asylum and refugee policy;
- Confidentiality and communication;
- Publicity;
- Applications for revision;
- Appeal, remedies, redress;
- Impact of CCF decisions and repeated requests;
- Impartiality of and public confidence in the CCF.

The ECBA's recommendations refer, *inter alia*, to the following:

- Doing more regular and consistent updates on case progress or enhanced communication channels;
- Implementing an amended process of disclosure of information, and revising the Operating Rules, so that it is ensured that an applicant has the ability to comment on an National Central Bureau's (NCB's) reasons for restrictions and achieves greater use of summaries in lieu of outright restriction;
- Ensuring more transparency and details regarding which information is shared between the CCF, the NCBs, and the Interpol General Secretariat (IPSG), including clearer rules on information processing within the IPSG;
- Establishing a review mechanism for wanted person diffusions similar to that applied for Red Notices;
- Reviewing the guidelines in order to assist applicants in identifying information that should not be disclosed and providing reasons for this;
- Reducing the overall number of revision applications by improving disclosure during the course of proceedings and introducing a right of appeal against CCF decisions;
- Establishing a formal monitoring mechanism to track whether NCBs implement deletion and correction decisions.

In addition, the report includes a number of recommendations on improving the CCF's internal organisation and strengthening its independence. Lastly, the ECBA expressed its hope that the report will feed into the further discussions on the reform of the CCF. It stressed that any reform of the CCF statute should not proceed in a piecemeal fashion and a thorough consultation of any further reform process should take place.

Based on the ECBA's February 2026 report, the ECBA & LATR provided a further statements on the proposed reform of the CCF statute in March 2026. The statement urge INTERPOL

to prioritise procedural fairness and equality of arms for individuals over new obligations for applicants. (TW)

Judicial Cooperation

ECJ: Speciality Rule in TCA is No Refusal Ground

On 23 April 2026, the ECJ held in Case C-528/24 (Boothnesse) that a possible infringement of the speciality rule – a basic concept in extradition law – by the issuing State does not constitute, in itself, a ground for the executing judicial authority to refuse the execution of an extradition arrest warrant.

➤ *Background of the case and question examined*

In the dispute in the main proceedings, three defendants objected to their extradition from Ireland to the United Kingdom (UK) on the ground that the arrest warrant issued for the prosecution of fraud did not include their conviction for contempt of court, as the defendants had failed to comply with restraint orders; the UK court had imposed an imprisonment of six months on each defendant for this act. However, according to the UK authorities, „contempt of court" is classified as a civil matter and not as a criminal offence, therefore, the arrest warrant could not include this act.

Given a reference for preliminary ruling from the Irish Supreme Court, the ECJ had to examine whether, in such situations, Art. 625 of the Trade and Cooperation Agreement concluded between the EU and the United Kingdom of Great Britain and Northern Ireland (TCA) requires or permits the Irish judicial authority to refuse the execution of the UK arrest warrant. Art. 625 TCA governs the speciality rule in cross-border extradition and surrender proceedings between EU Member States and the UK. It ensures that a surrendered person is not prosecuted, sentenced, or detained for any offense committed prior to their surrender, other than the specific crime for which they were handed over. For further details →eucrim 4/2025, 282–283 summarising the Advocate General's opinion in the case.

➤ *The ECJ's decision and reasoning*

According to the ECJ, the fact that the requested persons who are the subject of arrest warrants issued on the basis of the TCA with a view to bringing criminal prosecutions for a criminal offence has been sentenced, in the issuing State, to a penalty involving deprivation of liberty for another offence, which is not the subject of that arrest warrant, does not permit, in itself, the competent judicial authority to refuse to execute that arrest warrant. This follows from a literal, contextual and teleological interpretation of the provision:

- The wording of Art. 625 TCA does not indicate that the executing judicial authority is required, before ruling on the surrender of the requested person, to check whether the authorities of the issuing State are required to comply with the speciality rule or whether those authorities in fact comply, in practice, with that rule;
- The extradition refusal grounds are set out in Arts. 600 and 601 TCA which do not include a reference to Art. 625 TCA;
- Allowing the executing judicial authority to conduct a general review of whether the issuing authorities upheld the requirements of the TCA would impede the efficiency of the surrender mechanism established by the TCA.

However, the ECJ acknowledged that the infringement of the speciality rule must be seen in the context of the right not to execute an arrest warrant if there are valid reasons for believing that there would be a real risk to the protection of that person's fundamental rights if he or she were surrendered to the United Kingdom (Arts. 524(2), 604 lit. c) TCA). The fundamental rights in Art 47 CFR would be infringed, for example, if the requested person did not have, in the issuing State, any legal remedy enabling him/her to invoke an alleged breach of the speciality rule. It is finally for the referring court to examine whether the requested persons' fundamental rights risk to be infringed in the UK. (TW)

European Arrest Warrant

ECJ: Executing Member State Must Ensure Enforcement of Custodial Sentence if it Denies Surrender due to Fundamental Rights Grounds

spot light

If an EU Member State refuses the surrender of persons due to bad detention conditions in the EU Member States that sentenced them, the refusing Member State is required to enforce the prison sentence on its own territory. The main aim must be to avoid impunity of the requested person. This is the key statement of the Grand Chamber of the ECJ in its judgment of 4 June 2026 in the Joined Cases C-722/23 (Rugu) and C-91/24 (Aucroix).

➤ *Background of the cases and legal question*

In the dispute of the main proceedings, the Belgian courts refused to surrender a Romanian national residing in Belgium and a Belgian national to Romania and Greece respectively in accordance with Art. 1(3) of the Framework Decision 2002/584/JHA on the European arrest warrant (FD EAW) in conjunction with the ECJ case law in *Aranyosi and Căldăraru* (Joined Cases C-404/15 and C-659/15 PPU (→eucrim 1/2016, 16)). They argued that the EAWs from Romania and Greece, which sought to enforce custodial sentences against the defendants, could not be executed due bad detention conditions which would infringe the defendants' fundamental rights under Art. 4 CFR.

The referring Belgian Court of Cassation asked the ECJ what consequences the refusal would have for

the enforcement of the Romanian and Greek verdicts imposing custodial sentences. In particular, it wished to know whether the Belgian judicial authorities may, or even must, apply in addition the ground for optional non-execution provided for in Art. 4(6) FD EAW in order to prevent the impunity of the requested persons. Pursuant to Art. 4(6) FD EAW, an executing judicial authority *may* refuse to execute the EAW if that warrant has been issued for the purposes of enforcing a custodial sentence or detention order, where the requested person is staying in, or is a national or resident of, the executing Member State and that State undertakes to enforce the sentence or detention order in accordance with its domestic law.

For details →eucrim 2/2025, 151 summarising the opinion of Advocate General (AG) *Rantos* in the present case.

➤ *The ECJ's decision and reasoning*

The judges in Luxembourg first held that the optional refusal ground of Art. 4(6) FD EAW cannot be applied as a complement to the ground for mandatory non-execution resulting from Art. 1(3) FD EAW. The opposite approach would disregard the objectives pursued by each of those grounds as well as their respective nature.

However, the ECJ acknowledged that the EAW mechanism, which seeks to combat the impunity of a person requested for extradition who is present in a territory other than that in which he or she has committed an offence, must be respected. To this end, an executing authority that refuses to execute an EAW on fundamental rights grounds is required actively to seek to ensure that the requested person does not go unpunished as a result of that refusal. Therefore, the question raised in the present case must be resolved on the basis of Framework Decision 2008/909/JHA on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union (FD 2008/909).

The ECJ provides several clarifications on how FD 2008/909 should be applied in the present situation. These include:

- The objective of FD 2008/909 to increase the requested person's chances of reintegrating into society must be reconciled with the objective of FD 2002/584 to combat impunity;
- The executing judicial authority must apply FD 2008/909 in order to obtain recognition, in its territory, of the judgment imposing the sentence, delivered in the issuing Member State, which justified the issue of the EAW and, on the basis of that recognition, to ensure the enforcement of that sentence in that territory;
- In accordance with Art. 4(5) FD 2008/909, the executing authority must, on its own initiative, request the issuing Member State to forward the criminal judgment to it, together with the necessary certificate;
- When exercising discretion to refuse such transmission of the judgment, the issuing Member State must take due account of the fact that, as a result of that refusal, the sentenced person would remain unpunished;
- The judicial authorities involved must finally respect Art. 6(2) FD 2008/909 which provides for exceptions to the requirement for the convicted person's consent to the enforcement of the sentence in his/her home country or country of residence.

➤ *Put in focus*

The reasoning of the ECJ's Grand Chamber differs from the approach chosen by AG *Rantos* in the present case (→eucrim 2/2025, 151). The AG advocated for the application of Art. 4(6) FD EAW in addition to Art. 1(3) FD EAW. While the AG also applied FD 2008/909, he stressed the connection between Art. 4(6) FD EAW and the FD 2008/909, as set out in Art. 25 FD 2008/909. While the AG reached the result by advocating that the refusing Member State is required to enforce the sentence against the requested person on its own territory following a refusal to execute an EAW due to fundamental rights grounds on the basis of Art. 1(3) FD EAW, the ECJ appears more lenient requiring „only" that the executing Member State must „actively seek" the enforcement of the custodial sentence on its territory by way of applying FD 2008/909 exclusively.

Both, the ECJ and the AG adhere, however, to the case law that the avoidance of impunity is one of the Union's primary objectives. This objective is included not only in the EAW mechanism, but also in the founding treaties, as Art. 3(2) TEU offers the Union's citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured alongside appropriate measures to prevent and combat crime. The judges in Luxembourg explicitly stress this again.

Furthermore, the ECJ's judgment in *Rugu* and *Auctroix* reiterates the need for loyal cooperation between the judicial authorities of the EU Member States that operate in this area of freedom, security and justice. According to the ECJ, this cooperation must inform the dialogue between the executing and issuing authorities in order to ensure that the operation of the EAW is not brought to a standstill. (TW)

ECJ: Execution of EAW if Offence Was Committed Also in the Territory of Executing State

In its judgment of 12 February 2026 in Case C-712/25 PPU (Rastoshev), the ECJ ruled that the executing authorities cannot automatically refuse the execution of a European Arrest Warrant (EAW) if the offence has been committed in whole or in part in the territory of the executing Member State. This was the first time that the

ECJ had delivered an interpretation in respect of the optional refusal ground of Art. 4(7) of Framework Decision 2002/584/JI (FD EAW). Pursuant to Art. 4(7)(a) FD EAW, the executing judicial authority may refuse to execute the EAW where it relates to offences which are regarded by the law of the executing Member State as having been committed in whole or in part in the territory of the executing Member State or in a place treated as such.

➤ *Background of the case and question referred*

The main proceedings concern the execution of an EAW in Bulgaria. The EAW was issued by the Court of Marseille, France, against Bulgarian national XM for the purpose of prosecuting several offences allegedly committed between 2018 and 2024. Those offences were committed within the framework of an international criminal organisation with the aim of rigging sports competitions and took place in the territory of multiple Member States, including France and Bulgaria. The referring *Sofiyski gradski sad* (Sofia City Court, Bulgaria) has doubts as to whether it can refuse the surrender on the basis of Art. 4(7)) (a) FD EAW. It points out the existence of two divergent lines of case law regarding the interpretation of the provision transposing Art. 4(7)(a) FD EAW into Bulgarian law. According to the first line of case law, the fact that the offence was committed, in whole or in part, in the territory of Bulgaria cannot, in itself, justify a refusal to enforce the sentence; rather, an overall assessment must be carried out. Conversely, according to the second line of case law, such a circumstance should be regarded as sufficient grounds to refuse execution, since the Bulgarian Criminal Code is applicable to all offences committed in the territory of that Member State, without exception. The Sofia court wondered which line of case law complies with the FD EAW.

➤ *The ECJ's decision and reasoning*

At the outset, the ECJ recalled that Art. 4 FD EAW sets out optional refusal grounds. Depriving executing Member State's judicial authorities of the possibility to have a margin of discretion would substitute the mere option to refuse with a genuine obligation, even though the refusal of an EAW constitutes the exception, the execution of the EAW being the general rule.

As regards specifically Art. 4(7)(a) FD EAW, the judges in Luxembourg noted that the Union legislature intended to allow the person who is the subject of an EAW issued for the purposes of conducting a criminal prosecution, to be prosecuted by the authority in the most appropriate position for the proper administration of criminal justice.

Furthermore, a refusal solely on the ground that the offence in question was also committed in the territory of the executing Member State, without considering the specific circumstances of each case, would undermine the objective of the EAW mechanism: ensuring that perpetrators do not remain unpunished in the area of freedom, security and justice. This objective is also included in Art. 3(2) TEU.

In conclusion, the application of the ground for non-execution set out in Art. 4(7)(a) FD EAW should be left to the discretion of the executing judicial authority. This applies a fortiori where the offences giving rise to the EAW form part of a complex international criminal organisation affecting the territories of multiple Member States.

Lastly, the ECJ clarified the circumstances that the executing judicial authority must take into account in its assessment. These include, *inter alia*:

- The nature and characteristics of the offence;
- The international dimension of the offence(s);
- The place where the damage resulting from that offence materialised;
- The progress of the criminal proceedings in the issuing Member State and, depending on the case, in the executing Member State.

As a result, Bulgarian law interpreted in the sense that the fact that the offence, for which an EAW was issued for the purposes of conducting a criminal prosecution, was committed, in whole or in part, on the territory of the executing Member State (here: Bulgaria) is insufficient ground for refusing the execution of the EAW. (TW)

Trackathon to Locate Fugitives

On 3 and 4 June 2026, nearly 100 investigators and open-source intelligence (OSINT) specialists from 31 countries gathered at Europol headquarters for the 2026 edition of the ENFAST Trackathon. This event was a highly focused, high-intensity operation aimed at tracking down some of the most dangerous fugitives currently at large across Europe. The initiative concentrated specifically on high-priority cases that were nominated by the European Network of Fugitive Active Search Teams (ENFAST), working in close collaboration with member countries to identify and target these elusive criminals.

The operation was designed to focus on individuals who have successfully managed to avoid arrest despite extensive and ongoing efforts by national Fugitive Active Search Teams (FAST) dedicated to locating and apprehending them. Each of these fugitives is subject to a European Arrest Warrant, which authorizes their capture and extradition across member states. The coordinated effort aimed to close the gaps in enforcement and bring these fugitives to justice.

By employing advanced OSINT and social media intelligence techniques, the participating teams worked collaboratively and intensively to trace fugitives who continue to evade justice across national borders. FAST intervention teams stationed throughout Europe re-

mained on high alert and ready to mobilise at any moment, prepared to act immediately if a fugitive was successfully located through the intelligence gathered during the operation.

Out of the 57 high-level fugitive cases under review during the operation, new investigative leads were identified in 56 cases, demonstrating the effectiveness of the collaborative effort. In 26 of these cases, investigators were able to obtain valuable information regarding the possible whereabouts of the fugitives, and these leads will now be actively pursued by FAST teams to secure arrests and bring these individuals to justice. (CR)

Transfer of Sentenced Persons

ECJ: No Automatic Refusal to Enforce *in absentia* Convictions

On 21 May 2026, the ECJ delivered its judgment in Case C447/24 (Höldermann) concerning the recognition and enforcement of a custodial sentence imposed following a trial at which the sentenced person did not appear in person in the issuing State (in absentia conviction). Interpreting Art. 9(1)(i) of Framework Decision 2008/909 as amended by Framework Decision 2009/299/JHA, the Court first held that a sentenced person can be regarded as "aware of the scheduled trial" where the summons was served on defence counsel authorised both to conduct the defence and to accept service in the issuing State.

Second, the ECJ confirmed that Art. 9(1)(i) establishes an optional ground for non-recognition. Member States therefore cannot require recognition and enforcement to be refused solely because none of the situations expressly listed in that provision has been established.

Third, in such cases, the executing authority must remain able to assess, in the light of all the circumstances, whether recognition and enforcement would nevertheless be compatible with the sentenced person's rights of defence. In this assessment, the executing authority must take into account, among other factors, that the person personally requested enforcement in the Member State of his/her nationality and where he/she has his/her centre of interests.

➤ *Background of the case and questions referred*

Under Art. 9(1)(i) of Framework Decision 2008/909/JHA on the mutual recognition of custodial sentences, as amended by Framework Decision 2009/299/JHA, the executing State may refuse to recognise and enforce a judgment following a trial at which the sentenced person did not appear in person. The person's absence cannot, however, justify refusal where the case falls within one of three situations:

- The person was personally summoned or otherwise officially informed in due time of the date and place of the trial (point (i));
- The person, aware of the scheduled trial, had instructed a legal counsellor who represented him or her at it (point (ii)); or
- The person, after being served with the decision and informed of the right to a retrial or appeal, expressly accepted the decision or did not request a retrial or appeal within the applicable time frame (point (iii)).

The German implementation law (Section 84b(1) no. 2 of *the Gesetz über die internationale Rechtshilfe in Strafsachen* (*IRG*, Law on international mutual legal assistance in criminal matters)) turns the optional ground for non-recognition of the Framework Decision into a mandatory bar outside those situations.

SO, a German national, was sentenced by a Polish court in 2019 to one year's imprisonment for participation in an organised criminal group; his appeal was dismissed in 2022. He attended only a small number of the numerous first-instance hearings held over more than four years and did not appear at the appeal hearing, where a lawyer from his instructed defence counsel's firm represented him. Having designated his counsel's professional address as his address for service in Poland, the summons to the appeal hearing was duly served at this address.

At SO's request, the Polish court transmitted the judgment to Germany for enforcement, as Germany is both his Member State of nationality and the centre of his interests. However, the *Landgericht Berlin* (Regional Court, Berlin) refused the Berlin prosecutor's application for declaration of enforceability, holding that SO had neither been properly summoned to nor represented at several first instance hearings. At appeal, the *Kammergericht Berlin* (Higher Regional Court, Berlin, Germany) considered that SO's conduct could weigh in favour of recognition and enforcement, but believed that Section 84b IRG leaves no discretion to take such circumstances into account. In its reference for preliminary ruling, the *Kammergericht* sought guidance from the ECJ on the following issues:

- Whether service of the summons on a legal counselor instructed both to conduct the defence and to accept service can satisfy the requirement that the person concerned was aware of the scheduled trial;
- Whether the person must already know the scheduled date and place of the hearing when instructing that lawyer or whether it is sufficient that those details are communicated in due time before the hearing;
- Whether Art. 9(1)(i) of Framework Decision 2008/909 (as amended) precludes Section 84b(1) no. 2 IRG, which requires recognition and enforcement to be refused where the person did not appear at the relevant hearing unless one of the statutory exceptions applies;
- Whether, where none of the situations listed in Art. 9(1)(i)(i)–(iii) of the Framework Decision applies, the exe-

cuting authority can take into account that the person concerned personally requested enforcement in the Member State of his or her nationality and centre of interests.

➤ *The ECJ's reasoning on service and knowledge of the scheduled hearing*

As regards the first question, the ECJ held, by analogy with its judgment in *Kachev* (C-135/25 PPU), that service of the summons at the professional address of legal counsel authorised both to conduct SO's defence and to accept service was tantamount to informing SO personally and therefore satisfied the awareness requirement in Art. 9(1)(i)(ii) of Framework Decision 2008/909 (as amended). In such circumstances, recognition and enforcement do not infringe the rights of the defence or the rights to an effective remedy and a fair trial guaranteed by Arts. 47 and 48(2) of the EU Charter of Fundamental Rights, since SO can be regarded as having voluntarily and unequivocally waived his right to appear in person.

On the second question, the ECJ clarified the temporal relationship between the mandate and the person's awareness of the scheduled hearing. The different language versions of Art. 9(1)(i)(ii) leave open whether "awareness" must relate to the specific date and place of the hearing or merely to the fact that a trial will take place. Consistently with point (i) of the same provision and Art. 8(2) of Directive 2016/343, the judges in Luxembourg held that the person concerned must be informed in due time of the scheduled date and place of the hearing. This information need not, however, have been available when the mandate to the legal counsellor was conferred. Requiring knowledge of the hearing date at the time when the defence counsel was instructed would impose an excessive formal requirement and could require a mandate covering the entire proceedings to be confirmed or renewed once the hearing was scheduled. This would be particularly impracticable in appeal proceedings, where the counsel will generally be instructed before the date and place of the hearing are known.

➤ *The ECJ's reasoning on the optional character of the ground for non-recognition*

Regarding the third question, the ECJ emphasised that Art. 9(1)(i) of Framework Decision 2008/909 is drafted in permissive terms, providing that the executing authority "*may*" refuse recognition and enforcement. Referring to its case law on the identically worded Art. 4a(1) of the Framework Decision on the European Arrest Warrant, the ECJ held that Art. 9(1)(i) exhaustively and uniformly defines the circumstances in which a judgment rendered in the person's absence must nevertheless be recognised and enforced. Accordingly, where one of the situations listed in points (i)–(iii) is established, refusal on that ground is precluded; but where none applies, refusal remains optional rather than mandatory.

National legislation that converts this discretion into an automatic bar to recognition and enforcement, such as Section 84b(1) no. 2 IRG, prevents the executing authority from assessing, in the light of all the circumstances of the individual case, whether the person's rights of defence were nevertheless respected. Such legislation is therefore incompatible with Art. 9(1)(i). The executing authority must interpret this domestic law as far as possible in conformity with the wording and purpose of Framework Decision 2008/909, without adopting an interpretation *contra legem*.

➤ *The ECJ's reasoning on the factors for exercising discretion*

According to the ECJ, a request by the sentenced person for enforcement of the sentence in the Member State of his or her nationality and centre of interests does not, in itself, constitute a waiver within the meaning of Art. 9(1)(i)(iii) of Framework Decision 2008/909 (as amended), as it does not necessarily demonstrate that the person has relinquished any available right to challenge the conviction.

It can nevertheless be taken into account as part of the overall assessment of whether recognition and enforcement would impair the rights of the defence. Together with the sentenced person's conduct more generally, the request may be regarded as an indication that recognition and enforcement would not impair those rights, even where none of the situations expressly listed in points (i)–(iii) of Art. 9 of the Framework Decision has been established.

➤ *Put in focus*

In *Höldermann*, the ECJ transposed its interpretation of Art. 4a(1) of the Framework Decision on the European Arrest Warrant to the instrument on mutual recognition of custodial sentences (identically worded Art. 9(1)(i) of Framework Decision 2008/909). This parallel is particularly close, as both provisions were introduced by Framework Decision 2009/299 with the aim of harmonising the rules governing decisions rendered following a trial at which the person concerned did not appear in person.

The situations expressly listed in Art. 9(1)(i) therefore define the circumstances in which refusal based on the person's absence is precluded, but the ECJ clarified that they do not impose an obligation to refuse recognition and enforcement where the requirements could not be established. In such cases, the executing authority must retain discretion to assess, in the light of all the circumstances of the individual case, whether recognition and enforcement would nevertheless be compatible with the person's rights of defence. The Court adopted the same interpretation in its parallel judgment delivered on the same day in *Khuzdar* (C95/24), following a reference from an Italian court. (JK)

Council of Europe

Reported by Thomas Wahl (TW) and Joscha Kanstinger (JK)

Foundations

Human Rights Issues

Committee of Ministers: Declaration on the ECHR and Migration

On 15 May 2026, at the 135th session of the Committee of Ministers in Chişinău, Moldova, the foreign ministers of the 46 Council of Europe member states adopted, by consensus, a political declaration on the European Convention on Human Rights (ECHR) and migration.

The Declaration follows the informal Conference of Ministers of Justice held in Strasbourg on 10 December 2025, where ministers called for a common European approach to addressing contemporary migration-related challenges within the framework of the Convention. The Declaration was initiated by CoE's Secretary General *Alain Berset*.

The Declaration reaffirms the CoE member states' commitment to the Convention and their support for the independence of the European Court of Human Rights, underscoring that migration-related challenges require a coordinated response firmly rooted in human rights, democracy, and the rule of law. To this end, the ministers agreed to pursue these discussions within the Council of Europe's Network of Focal Points on Migration. The Declaration addresses the following key issues:

- **Immigration control and border protection:** The Declaration reaffirms states' sovereign right to determine their immigration policies, regulate the entry and residence of foreign nationals, and protect their borders, while emphasising that all such measures must be implemented in full compliance with the Convention.
- **Expulsion and extradition:** The Declaration acknowledges that the inability to expel or extradite individuals charged with or convicted of serious offences can lead to significant challenges for member states. While reaffirming the absolute nature of the prohibition of torture and inhuman or degrading treatment under Art. 3 ECHR, it stresses that the minimum level of severity required to engage that provision should remain "high and constant" and be applied clearly and consistently, so as to avoid unnecessary constraints on expulsion and extradition decisions. It further states that differences in the quality of accessible healthcare in the receiving state should preclude removal only in very exceptional circumstances. With regard to the expulsion of foreign nationals convicted of serious offences, the Declaration emphasises that, when assessing such measures under Art. 8 ECHR, national authorities enjoy a margin of appreciation in balancing the individual's right to respect for private and family life against the interests of national security and public safety.
- **Mass arrivals:** The Declaration acknowledges the particular pressure that large-scale arrivals place on frontline states and calls for enhanced operational cooperation to prevent irregular migration, facilitate returns, and combat the human trafficking and migrant smuggling networks involved, while ensuring full compliance with the Convention.
- **Instrumentalisation of migration:** The Declaration further addresses situations in which hostile states or other actors deliberately facilitate or exploit migratory movements to exert pressure on, destabilise, or undermine European states and their democracies. While reaffirming that the migrants concerned remain entitled to the protection of the Convention, it notes that both their conduct when attempting to cross a state border irregularly and the broader context of an orchestrated migratory movement may be relevant when assessing the state's compliance with its Convention obligations. In this context, the Declaration also refers to the ECtHR's concept of a "democracy capable of defending itself."
- **Decision-making and new approaches:** The Declaration calls for migration-related decisions to be taken through fair, clear, predictable, and timely procedures, with access to effective remedies and judicial oversight. Even when accelerated procedures are used to process large numbers of applications, the principle of individualised decision-making must be preserved. At the same time, it recognises that states may pursue "new approaches" to address and potentially deter irregular migration. Such approaches may include processing applications for international protection in third countries, establishing third-country "return hubs", and cooperating with transit countries, provided that states continue to fulfil their obligations under the Convention.

The ministers concluded by inviting the Secretary General to support activities aimed at strengthening national implementation, capacity-building, and

co-operation among member States and other stakeholders in line with this Declaration. The sharing of best practices should be promoted. (JK)

Committee of Ministers Gave Green Light to CoE Action on Information Manipulation and Foreign Interference

At their 135th session in Chişinău, Moldova, on 14–15 May 2026, the Committee of Ministers instructed the Secretary General to submit proposals for negotiations on a legal instrument addressing foreign information manipulation and interference (FIMI), including the possible establishment of a framework convention.

The initiative follows on from the Secretary General's 2026 report "*The New Democratic Pact for Europe in times of rupture*", which stressed the importance of boosting democratic security. FIMI encompasses covert, coordinated, or deceptive activities undertaken by foreign actors with the aim of shaping the information environment in ways that undermine democratic discourse, public trust, and the integrity of electoral processes. Building on a feasibility study submitted to the Committee of Ministers, the initiative reflects the ministers' assessment that such operations pose a substantial threat to the protection of human rights, the functioning of democratic institutions, and the rule of law.

The aforementioned study was prepared by the Committee of Experts on Foreign Information Manipulation and Interference (PC-FIMI), which was mandated, under the authority of the European Committee on Crime Problems (CDPC), to assess the feasibility of establishing such an instrument (→eucrim 3/2025, 212). The work reflects a changed geopolitical environment, shaped in particular by Russian information operations linked to its aggression against Ukraine, as well as the fragmented national responses to an inherently cross-border threat. Against this background, the study concludes that a common Council of Europe instrument is feasible and could establish a shared understanding of FIMI, strengthen societal and media resilience, improve detection and coordination, and enhance international cooperation.

The legal form and precise scope of a future instrument, however, remain open. At the CDPC's 89th plenary meeting in June 2026, delegations expressed divergent preliminary views, with some favouring a non-binding recommendation and others supporting a framework convention or another legally binding instrument (→eucrim news of 30 July 2026). The appropriate role of criminal law is similarly unsettled. The study emphasised that criminalisation should be considered only as a measure of last resort and that any response must safeguard freedom of expression and comply with the principles of legality, necessity, and proportionality. (JK)

Institutions

European Committee on Crime Problems (CDPC)

89th CDPC Plenary Meeting: Main Results

This news item continues the reporting of key decisions taken and main issues discussed by the European Committee on Crime Problems (CDPC). The CDPC oversees and coordinates the Council of Europe's activities in the field of crime prevention and crime control. The CDPC meets twice a year in plenary at the headquarters of the Council of Europe in Strasbourg (France). The 89th plenary meeting was held from 9 to 11 June 2026 under the Chairmanship of *Lorenzo Salazar* (Italy).

The CDPC welcomed the forthcoming opening for signature of the Additional Protocol to the Council of Europe's Anti-Money Laundering / Countering of Financing of Terrorism Convention – the Warsaw Convention (CETS No. 198). The opening for signature of the Additional Protocol is scheduled for 14 October 2026 in Strasbourg, after approval by the CDPC at its November 2025 plenary meeting (→eucrim 3/2025, 212) and subsequent adoption by the Committee of Ministers in Chișinău on 15 May 2026. The Additional Protocol will supplement and update the Convention in light of international regulatory developments. It extends the scope of asset recovery tools and mechanisms provided for in the Convention, aligning them with standards developed in other fora, such as the Financial Action Task Force (FATF) and the EU, and strengthening the powers of competent authorities in the field of asset recovery and international co-operation.

The CDPC also celebrated the launch of the Recommendation on accountability for technology-facilitated violence against women and girls, which was jointly prepared by the CDPC and the Gender Equality Commission (GEC) and adopted by the Committee of Ministers on 4 March 2026 (CM/Rec(2026)2). The Recommendation provides guidance to CoE member states by proposing a comprehensive approach to foster an environment of accountability in which technology facilitated violence against women and girls is neither facilitated, condoned, accepted nor ignored. The Recommendation expands beyond criminal law and also includes measures of civil and administrative law.

The Dutch delegation initiated discussions on the possible way forward with regard to the misuse of fireworks and pyrotechnics. Several delegations reported that fireworks and pyrotechnics are increasingly used by criminal organisations to create public disorder and intimidate others, including law enforcement.

Delegations also held an exchange of views on the nature of the future Council of Europe instrument on foreign information manipulation and interference (FIMI). The views expressed ranged from a framework convention, a recommendation, to a binding instrument.

The CDPC also took note of the progress in the following areas:

- Practical tools and guidance regarding the operation of European Conventions in criminal matters and accession of non-CoE member states to these conventions;
- With regard to penological issues, the draft recommendation on foreign nationals in prison, and the SPACE I statistics report of May 2026;
- The preparations of a Recommendation on deterring and fighting the smuggling of migrants (SoM) that will address the criminalisation of SoM, the protection and assistance for smuggled migrants, prevention, and international cooperation; it will also include sections on the financial dimension (a "follow-the-money" approach) and the digital dimension of SoM;
- The draft Recommendation on deepfakes within the Working Group of Experts on Artificial Intelligence and Criminal Law (CDPC-AICL);
- National practices on crypto assets with a focus on decentralised finance for financial crime investigations and asset recovery.

The agenda also included a comprehensive exchange of views on the topic of child-friendly justice, where delegations thoroughly discussed various issues highlighted in the gap analysis report. These issues encompassed the concerning growing trend in some member States towards lowering the age of criminal responsibility, the urgent need to effectively address situations in which children are exploited by adults to commit crimes, and the critical importance of implementing strong reintegration measures to support affected children. (TW)

Areas of Crime

Corruption

GRECO: Sixth Round Evaluation Report on Estonia

spot light

On 10 April 2026, GRECO published its newest report on Estonia. It is the first report of the sixth round of mutual evaluations, which focuses on preventing corruption and promoting integrity at the sub-national level. GRECO assesses in this round particularly the quality of governance and accountability of decentralised governments. The report on Estonia includes the municipalities of Tallinn and Tartu.

GRECO acknowledged Estonia's robust anti-corruption and integrity framework which is also evident at the municipal level. It also identified a number of good practices, such as Tallinn's and Tartu's public procurement arrangements, their anti-corruption clauses in contracts, e-training courses on anti-corruption and ethics for elected officials and municipal staff, access to official information, and participatory budgeting.

GRECO saw, however, room for improvement in several areas and addressed 12 recommendations to the Estonian authorities. In particular, these recommendations relate to the following:

- Looking at anti-corruption policy and risk management, the rules regarding the appointment of members of the supervisory boards of municipal companies and foundations should be reviewed;
- As far as standards of conduct and ethics are concerned, Tallinn and Tartu should equip counselling channels on integrity and ethics with clear confidentiality safeguards, raise awareness of these channels, and establish arrangements to clearly separate confidential advisory functions from the verification and investigation of integrity breaches;
- In the framework of conflict of interest prevention, practical guidance on the implementation of procedural restrictions under the Anti-Corruption Act and their relationship to criminal liability should be developed, and guidance on the exercise of secondary activities be clarified; measures should also be taken that strengthen the verification of declarations of interests;
- On transparency, access to information and public participation, citizen participation in decision-making should be strengthened, and lobbying be regulated at the central level through a clear framework;
- The subject of control mechanisms, oversight and accountability should be addressed by strengthening the human and administrative capacity of internal audit services, introducing appropriate safeguards for auditor independence and objectivity under rotation requirements, reviewing the protection of whistleblowers against CoE standards, and strengthening guidance, training, access to confidential advice and effectiveness monitoring.

Estonia was invited to report on the measures taken to implement the recommendations by 30 September 2027. (TW)

GRECO: Sixth Round Evaluation Report on Slovakia

In its second country report within the sixth round of mutual evaluations (focusing on the prevention of corruption at the sub-national level), GRECO acknowledged Slovakia a well-established anti-corruption and integrity system. This extends largely at the sub-national level, i.e., Bratislava and the Trenčín Self-Governing Region, which were assessed by GRECO's expert team. GRECO further states that both Bratislava and the Trenčin region have gone beyond the national framework and have developed a number of good practices. This includes ISO anti-bribery certification, transparency and integrity screening in the recruit-

ment of employees in managerial positions, the involvement of stakeholders in the preparation of codes of ethics, and procurement procedures. Yet, GRECO made 13 recommendations for areas in which further progress is needed. These recommendations include, for instance:

- Improving coordination between national and sub-national levels in the preparation and the implementation of national anti-corruption policy document;
- Analysing integrity and corruption risks on a regular basis;
- Introducing integrity safeguards for political officials, including mayors and presidents of self-governing regions, as well as for their deputies and advisers;
- Coupling codes of ethics and conduct (for Bratislava yet to be developed) with a credible supervision and enforcement mechanism, including specific and effective sanctions/measures for violations.

Other recommendations concern awareness-raising and enforcement measures, outside activities, post-employment restrictions, rules on gifts, the review of declarations of assets, liabilities and interests, lobbying and whistleblower protection.

GRECO invited the Slovak authorities to submit a report on the measures taken to implement the recommendations by 30 September 2027. GRECO will assess these measures by its specific follow-up procedure. (TW)

Money Laundering

MONEYVAL: Sixth-Round Mutual Evaluation Report on Latvia

spot light

On 19 February 2026, MONEYVAL published its sixth-round mutual evaluation report on Latvia. This is the first country report under the new, sixth evaluation round that started in 2024). It is the first country report under the new, sixth evaluation round, which started in 2024 (→eucrim 3/2024, 199 and →eucrim 3/2025, 214). This report is also the first evaluation worldwide conducted under the FATF's 2022 Methodology. Based on an on-site visit in November 2024, the report assesses the effectiveness of Latvia's system for combating money laundering (ML), terrorist financing (TF), and proliferation financing, as well as its compliance with the FATF Recommendations.

The report notes substantial progress since the fifth-round evaluation report in 2018 (→eucrim 2/2018, 109). The country's greatest money laundering risk no longer arises from its former role as a regional financial centre dominated by services for non-resident clients and significant cross-border financial flows. Instead, it is now primarily driven by domestic predicate offences – notably the shadow economy, fraud, and corruption – as well as by the growing risk of sanctions evasion linked to the EU measures adopted in response to Russia's war against Ukraine. This risk is heightened by Latvia's external EU borders with Russia and Belarus.

Against this background, MONEYVAL's principal findings and its effectiveness ratings for the FATF's eleven Immediate Outcomes (IOs) – key areas by which the effectiveness of a country's framework and actions to protect the financial system is measured and rated – can be summarised as follows:

➤ *Strengths*

- Risk understanding and financial intelligence: Latvia has a sound understanding of its ML/TF risks and benefits from effective inter-agency cooperation. The Financial Intelligence Unit, for instance, produces high-quality analysis that is widely used by law enforcement authorities (IO.1 and IO.6: high effectiveness).
- Financial supervision: Risk-based supervision has improved substantially, particularly in the banking sector. Enhanced supervision by *Latvijas Banka* has contributed to a significant reduction in financial-sector risks (IO.3: substantial effectiveness).
- Beneficial ownership: Latvia has established a robust framework for ensuring accurate and up-to-date beneficial ownership information. Data from the Enterprise Register and reporting entities are cross-checked, while competent authorities have timely access (IO.5: high effectiveness).
- Asset recovery: Asset recovery is a national priority and is assessed as highly effective (IO.8). Latvia seized more than €3 billion and confiscated over €300 million, primarily through non-conviction-based proceedings suited to complex cross-border cases.

➤ *Shortcomings*

- Non-financial-sector supervision: This is Latvia's most significant shortcoming. It is the only area rated as "moderately effective" (IO.4), and is the sole focus of MONEYVAL's Key Recommended Actions. Supervisory resources are not consistently targeted at the highest-risk sectors. In particular, oversight of lawyers remains weak due to limited resources, insufficient risk-based supervision, and low levels of suspicious transaction reporting.
- Legal persons and legacy cases: Legal persons are prosecuted too rarely, and the sanctions imposed are often insufficiently dissuasive. Many older "laundromat" cases could not be prosecuted because the offenders or beneficial owners were either unknown or located abroad.
- Asset recovery and international cooperation: Latvia seizes considerably more assets than it ultimately confiscates, largely due to lengthy judicial proceedings delaying final decisions; this is compounded by the comparatively limited use of international cooperation in corruption cases, despite effective engagement with foreign counterparts elsewhere.

Overall, Latvia achieved a high or substantial level of effectiveness in

ten of the eleven IOs, while all but one FATF Recommendation was rated as "Compliant" or "Largely Compliant". Consequently, Latvia was placed in the regular follow-up process and is scheduled to report back to MONEYVAL in June 2028. (JK)

MONEYVAL: Typologies Report on Financial Crime Risks Linked to Conflict-Related Proceeds

On 12 March 2026, MONEYVAL released a typologies report examining money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks linked to conflict-related proceeds. Adopted at MONEYVAL's 70th Plenary in December 2025 (→eucrim 4/2025, 289), the report is based on information from 17 MONEYVAL jurisdictions and recent case studies. It identifies key methods by which such proceeds are generated, moved, and concealed.

The report examines how armed conflicts and military aggression create conditions in which illicit proceeds are generated and laundered and may subsequently be used for terrorist or proliferation financing. MONEYVAL highlights that weakened state institutions, disrupted markets, and limited regulatory and law enforcement capacity allow conflict-related criminal economies to take root and spread across borders, thereby perpetuating conflict and instability.

The report's key findings can be summarised as follows:

- Conflict-related financial flows take many forms and frequently cross borders: The report identifies corruption, fraud, cybercrime, trafficking of drugs and arms, and the misappropriation of resources as important sources of conflict-related proceeds. These funds are then moved through a combination of formal and informal financial channels, corporate structures, and virtual assets, sometimes involving state-linked actors, mercenaries, or private military companies.
- Sanctions circumvention is a major conflict-related risk: MONEYVAL finds that such schemes are becoming increasingly sophisticated and transnational, particularly in the context of proliferation financing. They rely on shell and offshore companies, third-country intermediaries, and virtual assets to conceal ownership and financial flows. The cases examined range from concealed transactions involving military and dual-use goods to attempts to circumvent restrictions on virtual asset services.
- Conflict-related risks remain insufficiently reflected in national risk assessments (NRAs): Of the 17 responding jurisdictions, seven had not explicitly addressed conflict-related ML, TF, or PF risks in their latest NRAs, while four were updating them. Even where such risks were considered, key threats such as arms trafficking, cybercrime, and the activities of foreign fighters or private military companies often remained unassessed. Non-profit organisations (NPOs) illustrate this gap: although eight jurisdictions identified NPOs as vulnerable to TF abuse, only three had examined in depth the risks associated with NPOs and crowdfunding platforms in conflict zones.
- Risk-mitigation measures are expanding, but their implementation remains uneven: Jurisdictions increasingly use targeted financial sanctions, asset freezes, confiscation, financial intelligence, and cross-border cooperation to disrupt conflict-related financial flows. Yet, their effectiveness is hampered by weak inter-agency coordination, limited proactive use of financial intelligence, uneven sanctions monitoring, and insufficient private-sector engagement.

MONEYVAL therefore encourages its members to integrate conflict-related risks into national risk assessments, translating the findings into targeted action plans and supervisory indicators. It also calls for closer cooperation among competent authorities, across borders, and with the private sector, alongside the greater use of technological tools to trace financial flows. Ultimately, the report stresses the need to align financial supervision more closely with geopolitical risk analysis. (JK)

MONEYVAL: Updated Typologies Report on Use of Virtual Assets

On 10 February 2026, MONEYVAL published an updated typologies report on the misuse of virtual assets (VAs) and virtual asset service providers (VASPs) for money laundering, terrorist financing, proliferation financing, and sanctions evasion. Drawing on information from 25 jurisdictions, the report follows up on MONEYVAL's 2023 review (→eucrim 3/2023, 272). It reflects the rapid technological developments in crypto-assets and the wider virtual-asset sector, with a particular focus on the circumvention of targeted financial sanctions.

MONEYVAL records substantial progress since the 2023 review, finding that many of the regulatory and supervisory gaps identified at that time have narrowed considerably. Within the EU, this development has been reinforced by the Markets in Crypto-Assets Regulation (EU) 2023/1114 and the recast Transfer of Funds Regulation (EU) 2023/1113 in particular. Nevertheless, MONEYVAL finds that stronger regulatory frameworks have not yet translated into equally effective implementation and enforcement. The report highlights the following:

- Of the jurisdictions reviewed, 81% now require VASPs to be licensed or registered, and more than 90% have designated a competent supervisory authority. However, enforcement remains weak, particularly against unlicensed and offshore providers operating across borders.
- Only 46% of the reviewed jurisdictions had operationalised the FATF "travel rule", which requires VASPs to obtain and transmit identifying in-

formation on the originator and beneficiary of virtual asset transfers. Although the necessary legal frameworks are often in place, supervision, enforcement, and cross-border implementation remain underdeveloped.

- The circumvention of targeted financial sanctions has become a particular concern. Although VASPs are generally subject to the same sanctions obligations as other financial institutions, few jurisdictions have robust mechanisms for detecting and penalising violations. These shortcomings are compounded by national risk assessments that frequently pay insufficient attention to sanctions evasion and proliferation financing and by the limited availability of systematic data on cross-border virtual asset flows.
- Criminal uses of virtual assets are becoming more diverse and sophisticated, as is seen with investment and romance fraud, child exploitation, online-recruited money-mule networks, and proliferation financing by state-sponsored actors. Anonymity-enhancing services and complex transaction structures can obscure the movement of virtual assets and make criminal investigations more difficult.
- Reporting by VASPs has increased markedly, but its practical value remains limited. Among jurisdictions providing comparable data, 80% recorded an increase between 2022 and 2024. Reports are often generated automatically or filed defensively without adequate human assessment. MONEYVAL believes that fewer, more targeted reports would produce better financial intelligence and it identifies public-private cooperation as a means of improving reporting quality. Yet only 40% of jurisdictions currently have active initiatives involving VASPs.
- International cooperation appears to function well, with extensive exchanges taking place through FIUs, law-enforcement and supervisory networks. No jurisdiction reported legal barriers to providing assistance. Domestic operational capabilities, remain uneven, however. Some authorities still lack specialist expertise, blockchain-analysis tools, or established procedures for tracing and securing virtual assets, while foreign VASPs and decentralised platforms can hinder timely access to information and assets.

Overall, MONEYVAL calls on its members to sharpen national risk assessments, improve the quality of VASP reporting, and strengthen the expertise and tools needed to investigate and secure virtual assets. It also recommends clearer guidance for the sector and continued reliance on existing cross-border cooperation mechanisms. (JK)

Counterfeiting & Piracy

2026 MEDICRIME Conference: Call for Wider Accession to the MEDICRIME Convention

On 28 April 2026, high-level representatives from health, law enforcement, customs, and judicial authorities, as well as from international organisations and the private sector adopted conclusions on the MEDICRIME Convention. The Council of Europe's MEDICRIME Convention is the only international criminal law instrument aimed at preventing and combating threats to public health. It identifies activities endangering public health as criminal offences, protects victims' rights, and provides the basis for efficient national and international cooperation. It entered into force on 1 January 2016 (→eucrim 2/2016, 84–85; see also eucrim 1/2025, 40–41 and eucrim 4/2021, 233).

At a conference in Chișinău, organised by the Council of Europe together with the Agency for Medicines and Medical Devices of the Republic of Moldova's Ministry of Health, participants acknowledged the growing global threat posed by the falsification of medical products and related crimes. They pointed out that criminal networks are increasingly exploiting online sales, social media, encrypted apps, and e-commerce platforms to distribute falsified products. Of particular concern are lifestyle products, such as weight-loss and performance-enhancing drugs, which promise high profits for organised crime. At the same time, emerging technologies, including artificial intelligence, are being used to generate fake endorsements and testimonials. Other concerns include the falsification of veterinary medical products and the increasing circulation of illicit medical products in sports.

Against this backdrop, the conclusions include a number of recommendations for future actions, among other things:

- Strengthening the promotion of further accessions of State Parties to the MEDICRIME Convention;
- Strengthening the 24/7 Network on cooperation and information exchange;
- Addressing emerging threats through guidance and monitoring;
- Enhancing national multi-agency cooperation and expanding international partnerships.

Other priority areas include raising public awareness, particularly about the risks associated with online purchases, and strengthening victim protection and access to justice.

At the conference in Chișinău, the committee of parties to the MEDICRIME convention also adopted a new report on "The Medicrime Convention in the age of AI: challenges and opportunities". This report was prepared by Prof. *Fernando Miró Llinares* from the University Miguel Hernández of Elche (Spain). It evaluates the impact of AI on the applicability and relevance of the MEDICRIME Convention, and reflects on the need to update, reinterpret, or strengthen the provisions of the Convention considering the emerging challenges associated with AI. (TW)

Articles

Articles / Aufsätze

Fil Rouge

Over the past two decades, the European Union has emerged as a significant actor in shaping procedural safeguards, developing a common framework of defence rights intended to strengthen both mutual trust and the protection of fundamental rights. Yet, the implementation and practical effectiveness of these guarantees continue to raise important questions. The articles in this issue examine the evolution, current state, and future direction of procedural safeguards in European criminal justice. Although they address different aspects of procedural protection, they share a common concern: how to ensure effective rights protection in an increasingly integrated and technologically transformed European legal order? This question has acquired particular urgency in light of new forms of cross-border cooperation, the growing reliance on digital technologies and algorithmic tools, and evolving perceptions of security and risk, all of which challenge traditional understandings of fair trial rights and due process. Against this backdrop, the contributions gathered here critically assess whether existing safeguards remain fit for purpose and explore how they may need to evolve to preserve the legitimacy, fairness, and rights-based foundations of European criminal justice in the years ahead.

The issue opens with an analysis of the Office of the Controller of Procedural Guarantees within the European Anti-Fraud Office (OLAF). The article traces the evolution of accountability mechanisms in EU administrative investigations and their contribution to protecting individual rights. As OLAF's powers have expanded, the Controller has become an important safeguard at the interface between administrative and criminal enforcement.

The retrospective assessment continues with an in-depth examination of the jurisprudence of the Court of Justice of the European Union on three key procedural rights directives: the rights to interpretation and translation, the right to information, and the right of access to a lawyer. Based on a systematic review of the case law, the article demonstrates how the Court has strengthened the practical effectiveness of procedural rights while seeking to reconcile minimum harmonisation with the diversity of national criminal justice systems. At the same time, it identifies remaining inconsistencies and underscores the continuing challenges to mutual trust and effective rights protection in the Area of Freedom, Security and Justice.

Having reflected on past achievements, the issue then looks ahead to future challenges. Drawing on discussions at the High-Level Forum on the Future of EU Criminal Justice, the third contribution argues that future developments in EU criminal law should remain firmly anchored in the values enshrined in Article 2 TEU. In times of growing pressures on democracy, the rule of law, and fundamental rights, it advocates a value-based approach to legislative and policy development.

The subsequent two contributions bring the perspectives of legal practitioners into the debate. The contribution by the Council of Bars and Law Societies of Europe (CCBE) emphasises that mutual trust can thrive only where judicial independence, effective access to justice, professional secrecy, and defence rights are fully respected. Along similar lines, the European Criminal Bar Association (ECBA) calls for a renewed roadmap for defence rights to address persisting gaps in protection and to ensure that procedural guarantees keep pace with developments in European criminal justice.

The issue concludes with an examination of one of the most significant challenges facing contemporary criminal justice systems: digitalisation. The increasing use of large-scale data collection, algorithmic analysis, artificial intelligence, automated decision-making, and cross-border access to electronic evidence promises greater efficiency in law enforcement, but it also raises fundamental questions about transparency, accountability, judicial oversight, and the effective exercise of procedural rights. By examining the growing overlap between preventive and repressive measures, the article questions whether existing safeguards remain adequate in an environment characterised by continuous data processing and predictive technologies. It thereby offers a forward-looking agenda for preserving fundamental rights in the digital age.

Prof. Dr. Katalin Ligeti, University of Luxembourg & eucrim editorial board member

OLAF's Controller of Procedural Guarantees in the Twilight Zone between Procedural Fairness and Investigative Effectiveness

Julia Laffranque*

The function of the Controller of procedural guarantees was established in 2020 to ensure that the effectiveness in investigations conducted by the European Anti-Fraud Office (OLAF) does not come at the expense of fundamental rights and procedural guarantees. The Controller examines in an independent manner complaints submitted by persons concerned in OLAF investigations. This complaints mechanism has proved to be an effective remedy for persons concerned and also aims to increase the transparency and accountability of OLAF's activities.
In an effort to shed light on the function of the Controller of procedural guarantees, the complaints mechanism, and the delicate balance struck between procedural fairness and investigative effectiveness, this article reflects on the work carried out during Prof. Dr. *Julia Laffranque's* nearly four-year mandate as the first Controller of procedural guarantees. She presents some of the main achievements of the function and shares the lessons learnt from handling the complaints mechanism, as well as her vision for both the Controller's function and the complaints mechanism moving forward.

I. Introduction

The original OLAF Regulation's lack of a formal procedure for handling individual complaints by persons concerned had long cast doubt on the sufficiency of existing mechanisms to safeguard fundamental rights and procedural guarantees in all circumstances.[1] After a long legislative journey,[2] the gaps identified were finally addressed through Regulation (EU, Euratom) 2020/2223,[3] which amended Regulation (EU, Euratom) No. 883/2013 (the "OLAF Regulation")[4] and created the function of the Controller and the complaints mechanism. As this article further elaborates, experience since then has confirmed both the necessity of this function and its added value.

The Controller serves as an **independent safeguard** for persons concerned, i.e., persons or economic operators suspected of having committed fraud, corruption or any other illegal activity affecting the financial interests of the Union and who are therefore subject to investigation by OLAF.[5] The Controller was designed to reinforce the legitimacy, integrity, and public trust of OLAF's investigative activity. Having been appointed as the first Controller on 3 May 2022, I have since exercised my mandate by gradually but steadily adjusting and aligning the principles of effective judicial protection with those of administrative protection.

As *Lord Hewart* famously stated, "justice should not only be done, but should manifestly and undoubtedly be seen to be done.".[6] This principle is particularly relevant to administrative investigations, where the appearance of fairness is inseparable from institutional legitimacy. OLAF's investigative conduct must therefore be beyond reproach. Full respect for and safeguarding of the procedural guarantees and fundamental rights of persons concerned in its investigations are foundational to the credibility of OLAF's work.

The Controller handles complaints lodged by persons concerned regarding the Office's compliance with procedural guarantees, as well as complaints alleging infringements of the rules applicable to investigations by the Office,[7] in particular infringements of procedural requirements and fundamental rights.[8] To that end, a complaints mechanism was established.[9]

Since my appointment as Controller, I have dealt with more than 70 complaints and horizontal issues impacting the rights of persons concerned in OLAF investigations. In doing so, I have taken into account fundamental rights stemming from the Charter of Fundamental Rights of the EU (the Charter),[10] alongside the specific procedural guarantees that govern OLAF's activities, general legal principles, and the case-law of the EU Courts applicable to OLAF investigations. As a former judge of the European Court of Human Rights (ECtHR), I have also drawn on its case-law regarding fundamental rights guaranteed.[11]

I would also like to emphasise that, in my practice as Controller, I have given special consideration to the right of persons concerned to good administration. The right to good administration enshrined in Art. 41 of the Charter sets forth the right of every person to have his or her affairs handled

impartially, fairly, and within a reasonable time by EU institutions, bodies, offices, and agencies (IBOAs). I have thus consistently recalled in my decisions the importance of OLAF staff performing their duties in strict compliance with the core requirements of objectivity, impartiality, professionalism, procedural fairness, and respect for fundamental rights. I firmly believe that ensuring the impartiality and fairness of all OLAF activities not only protects individual rights but also reinforces the legitimacy and credibility of OLAF investigations themselves. This is how justice is not only done, but also seen to be done.

The complaints mechanism is an effective remedy for persons concerned to increase the transparency and accountability of OLAF's activities. I am convinced that the complaints mechanism has already become an essential safeguard for persons concerned and will further grow into its role in ensuring that OLAF's activities comply with the relevant procedural guarantees and the rules applicable to investigations.

I welcome the interest shown in other *eucrim* publications in my function and in developments in the protection of fundamental rights and procedural rights in OLAF investigations.[12] The aim of this article is to shed light on the function of the Controller and the complaints mechanism, reflecting on the work carried out during my almost four-year mandate. I have endeavored to ensure high standards of protection for the fundamental rights and procedural guarantees of persons concerned, while closely working with OLAF to improve the conduct of its investigations in constructive manner. The main achievements of this delicate exercise are presented in this article, where I also share some of the key lessons learnt from handling the complaints mechanism. Finally, I provide an outline of my vision for both the function and the complaints mechanism moving forward.

II. The Controller's Mandate

When applying the complaints mechanism, the Controller does not interfere with the conduct of an ongoing investigation, as this would constitute a breach of OLAF's independence.[13] The Controller also does not seek to substitute her own assessment for that of the OLAF Director-General on whether to open an investigation, the choice of investigative measures, the assessment of evidence, or the conclusions reached.[14]

Instead, the Controller's role involves providing administrative scrutiny to ensure that administrative discretion is exercised within the boundaries of legality, proportionality, and the principles of good administration. If the Controller finds that no breach of procedural guarantees or of the rules applicable to OLAF investigations has occurred, she **provides reassurance** to the complainant that OLAF has acted in conformity with the rules set out in its legal framework. Conversely, if the Controller finds a breach, she will invite OLAF to take action to resolve the complaint by making a **proposal for a solution.** If the Controller does not find the actions taken by OLAF satisfactory, he/she will make a **recommendation** to OLAF on how to resolve the complaint as a second step.[15]

As a rule, lodging a complaint does not have suspensive effects on the conduct of the underlying OLAF investigation.[16] Nevertheless, the Controller always strives to strike an appropriate balance between the need to safeguard the efficiency and continuity of OLAF investigations and the requirement to ensure effective protection of fundamental rights and procedural guarantees. In particularly sensitive cases, the Controller has requested that OLAF temporarily suspend its investigative activities while a complaint was under examination. Likewise, there have been instances in which OLAF suspended investigations on its own initiative upon receiving notification that a complaint had been lodged with the Controller. This has occurred in cases where complaints alleged shortcomings affecting the rights of defence, the legality of investigative measures, alleged conflicts of interest among members of the investigation team, and breaches of fundamental rights.

It is also important to clarify that there are three main oversight actors, each with complaints mechanisms, operating under distinct legal frameworks within the EU system of administrative accountability. Nonetheless, their mandates intersect at certain points:

- The **European Ombudsman**[17] examines complaints and conducts own-initiative inquiries into maladministration by IBOAs, without providing a substitute for judicial review.
- By contrast, the **Controller** of procedural guarantees is a specialised function embedded in the OLAF administrative investigations regime who handles complaints alleging breaches of the procedural rights applicable in OLAF investigations. This includes matters pertaining to the right to good administration under Art. 41 of the Charter. As a result, there may be complaints regarding alleged maladministration in the conduct of an OLAF investigation that could potentially be lodged simultaneously or subsequently before both the Controller and the European Ombudsman, while respecting their respective mandate and time limits.
- The **European Data Protection Supervisor** (EDPS) is an independent supervisory authority responsible for pro-

tecting the rights to privacy and to the protection of personal data .[18] Since the EU has created a dedicated body to guarantee the fundamental right to the protection of personal data, it is for the EDPS, rather than the Controller, to deal with complaints concerning alleged breaches of data protection rules.[19] While the Controller does not deal with allegations that purely concern the interpretation and application of the EU data protection rules, she considers aspects relating to privacy and data protection when assessing OLAF's overall compliance with procedural guarantees.[20]

III. Achievements of the Complaints Mechanism to Date

From the outset, the Controller has approached the function with the aim of contributing to the continuous improvement of OLAF's investigative practices. This objective has primarily been pursued through decisions adopted under the complaints mechanism, complemented by regular exchanges with OLAF counterparts.

Over time, the Controller has also developed a steady practice of including *obiter dicta* in her decisions. While these observations are not strictly necessary for resolving the individual complaint, they are intended to strengthen the overall protection of fundamental rights and procedural guarantees of the persons concerned, as well as to promote compliance with the rules applicable to OLAF investigations. Even in cases where no formal breach has been established, **these *obiter dicta* have played an important corrective and preventive role**. They have highlighted practical shortcomings, clarified interpretative uncertainties, and identified areas where adjustments to OLAF's internal practices (or, where appropriate, to the OLAF Regulation), may be warranted. In this way, the complaints mechanism has served as both a remedial tool and a driver for systemic improvement. Furthermore, in cases where complainants retained the services of specialised lawyers, the quality of the exchanges during the handling of their complaints indicates a deepening interest and understanding in the area of fundamental rights and procedural guarantees in the context of OLAF investigations among the legal community.

Since the establishment of the complaints mechanism in 2022, the Controller has handled 76 complaints. In four cases, proposals for a solution were addressed to the OLAF Director-General, all of which were accepted and implemented.[21] Beyond the resolution of individual complaints, the decisions adopted by the Controller have progressively shaped OLAF's investigative practices by clarifying the scope and practical application of procedural guarantees. In several instances, the legal reasoning developed in complaints decisions has directly informed amendments to the Guidelines on Investigation Procedures for OLAF Staff (the GIPs),[22] thereby extending the impact of individual cases beyond their immediate factual context.[23]

1. Admissibility of complaints

The admissibility of complaints serves as an important gatekeeping element in the complaints mechanism. The one-month time limit for lodging complaints in respect of closed investigations, pursuant to Art. 9b(2) of the OLAF Regulation[24], reflects a legislative choice aimed at preserving the effectiveness of subsequent judicial or administrative follow-up proceedings at national or EU level. However, the combination of this strict admissibility condition and the absence of a general obligation on OLAF to inform persons concerned of the closure of cases involving findings against them may result in instances where access to the complaints mechanism is *de facto* denied.[25]

Addressing this issue has been a key part of the Controller's casework. In one of the complaints lodged in 2025, she considered that the automatic application of Art. 9b(2), first subparagraph, second sentence, of the OLAF Regulation would, in the exceptional circumstances of the case, undermine the principles of fairness and good administration, as guaranteed by Art. 41 of the Charter. In the case at issue, OLAF had informed the complainant of the possibility of lodging a complaint with the Controller only after the one-month period had already elapsed. In this context, the Controller concluded that the only interpretation that would ensure the effectiveness of Art. 9b(2) of the OLAF Regulation was that OLAF intended for the notification of that communication to serve as the *dies a quo* of the limitation period. This interpretation ensured that the complainant was not, in practice, deprived of access to the complaints mechanism.

2. Fundamental rights

The first three years of the Controller's tenure have proved particularly fruitful, yielding tangible improvements in the handling of the fundamental rights and procedural guarantees in OLAF's investigations. During this time, the Controller has observed a gradual but steady improvement in OLAF's practices. This suggests that the guidance provided through her decisions on the content and practical operation of the rights of persons concerned in OLAF investigations has played a meaningful role in encouraging OLAF to strengthen its safeguards for these rights. The examples set out below illustrate some of the most significant ways

in which the Controller has contributed to clarifying and reinforcing these safeguards to date. They refer to the right to be informed, the requirement to give reasons under the right to good administration, the right to be heard in the framework of the opportunity to comment on the facts established by OLAF, and the right to be assisted by a person of choice during internal investigations.

During the first year of her activities, the Controller found a **breach of a complainant's right to be informed of the closure of an OLAF investigation with no findings** against them. According to Art. 11(7) of the OLAF Regulation and Art. 80(1) of the GIPs, OLAF is clearly obliged to inform the person concerned within 10 working days of the decision to close an investigation in which no evidence has been found against them. Upon completion of the investigation, OLAF found no evidence against the complainant and sent a notification, but **did not verify whether the complainant had effectively received it** (e.g., by requesting an acknowledgement of receipt). More than a year after the closure of the OLAF investigation and only after having requested access to the final report under Art. 10(3b) of the OLAF Regulation, the complainant finally received notification that no evidence had been found against them. In this case, the Controller did not make a proposal for a solution, as the complainant had obtained access to the final report while the complaint was being processed and had therefore become aware that no evidence had been found against them. Nevertheless, the Controller reminded OLAF that this was a serious breach and invited the Office to pay careful attention to similar cases in the future. In line with the Controller's *obiter dicta*, OLAF amended its internal procedures for notifying persons concerned and clarified this issue in the newly adopted GIPs.[26]

Regarding communications with persons concerned, in a different case the Controller acknowledged that the OLAF Regulation does not specify the means of communication OLAF should use in correspondence with persons concerned. However, she underscored that **OLAF must ensure that the means of communication used enable persons concerned effectively to become aware of the information sent to them by OLAF**. Furthermore, it is for OLAF to demonstrate that it has complied with its obligations and communicated the information in a way that could reach the person concerned. OLAF has a margin of discretion as to the means it chooses to send notifications to persons concerned. Thus, the Controller held that is for the investigative team to choose the means they deem most effective, as long as their purpose is attained. If the chosen means turns out to be ineffective, it is within the **discretion of the investigative unit to make use of any other available tool** in order to effectively inform the person concerned of a certain communication. In the case at hand, the Controller found that OLAF had acted diligently and in line with the applicable rules, and that no breach had occurred.

In various decisions, the Controller has held that **persons concerned do not enjoy an autonomous right to be interviewed**; the choice of investigative measures remains within OLAF's margin of discretion. However, in one case, the complainant challenged OLAF's refusal to hear additional witnesses whom they considered essential to the investigation. While recognising OLAF's discretion to determine the most appropriate investigative measures, the Controller emphasised that, pursuant to Art. 41 of the Charter, OLAF must provide clear and specific reasons when it decides not to conduct an interview requested by a person concerned.

In another case, the Controller examined OLAF's **refusal to grant access to documents referred to in the summary of facts**. The refusal was based solely on the absence of a general right of access to the investigation file. The Controller found that such reasoning was insufficient. OLAF must assess, in light of the right to be heard, whether the person concerned was effectively able to submit observations without access to the requested documents or knowledge of their content. Nevertheless, the Controller's decisions have consistently reiterated that no provision confers a general right of access to all documents requested by the person concerned.

Several complaints have raised allegations regarding the conduct of **inspections of premises during internal investigations in connection with the right to be assisted by a person of one's choice**. Unlike external investigations, where economic operators are afforded the right to be assisted by a person of choice and the privilege against self-incrimination during on-the-spot checks under Art. 3(8), the OLAF Regulation does not expressly recognize those rights for persons concerned in internal investigations. However, **the Controller has taken the view that, as a matter of good administrative practice, OLAF investigators should inform persons concerned in internal investigations that they are free to seek legal advice during inspections**. Furthermore, while the applicable legal framework does not prescribe a specific form for communicating the procedural rights of the person concerned in either internal or external investigations, the fundamental importance of those rights justifies consistently providing information about them **in writing**. The Controller has called for legislative action to further consolidate these best practices within the OLAF Regulation.[27]

3. Procedural guarantees

A recurring issue raised by complainants has been the **definition of the scope of investigations** and whether OLAF has acted beyond that scope. The Controller has consistently maintained that an overly broad definition of scope would risk undermining the principles of legality and proportionality that must be observed by OLAF at the selection phase.[28] This particularly concerns the assessment of whether there is sufficient suspicion[29] to open an investigation. OLAF took the Controller's considerations into account when amending the GIPs,[30] which now require the scope of an investigation to be clearly defined in the opening decision.

Another question raised before the Controller was whether OLAF could continue a **complementary investigation**[31] after the European Public Prosecutor's Office (EPPO) had closed a criminal investigation on the same facts due to insufficient evidence, or whether such continuation would infringe the ***non bis in idem* principle**. The complainant argued that the overlap between the two proceedings required OLAF to discontinue its investigation following the EPPO's decision. The Controller recalled that Art. 12f(1) of the OLAF Regulation expressly allows OLAF to conduct complementary investigations in parallel with EPPO proceedings and that the two proceedings inherently differ in nature and purpose: OLAF conducts administrative investigations which may lead to financial, judicial, disciplinary, or administrative recommendations, whereas the EPPO carries out criminal investigations that may result in criminal convictions. In line with the case-law of the EU Courts, the Controller held that the dismissal of the criminal investigation does not constitute a final determination of liability for the purposes of the *non bis in idem* principle and does not preclude administrative action, such as a complementary investigation by OLAF.

The Controller has also examined OLAF's practice of distinguishing between **the naming of a person concerned in the decision opening a case and the subsequent registration of that information in the OLAF case management system** (OCM), to which the Controller has privileged access.[32] It was found that this practice does not promote legal certainty, as it is not provided for in the applicable legislation,[33] and may breach the procedural rights of persons concerned in certain circumstances. This issue has been partially addressed in the revised GIPs, where the clarification of the status of the person concerned constitutes one of most significant amendments.[34]

Finally, the Controller addressed OLAF's handling of **comments submitted by persons concerned on the summary of facts**.[35] She held that a generic statement in the final report (according to which the comments provided by the person concerned did not alter the facts or OLAF's assessment thereof) is insufficient, taken in isolation, to demonstrate that those comments had been genuinely considered. OLAF has taken these considerations seriously and, in line with the Controller's suggestions, has implemented them into the new GIPs.[36]

IV. Changes and Challenges Ahead

In the context of the evaluation of the OLAF Regulation, and drawing on her extensive experience in handling the complaints mechanism, the Controller has issued an opinion on the application and impact of the provisions of the OLAF Regulation related to her mandate. This opinion identifies areas in which the protection of fundamental rights and procedural guarantees in OLAF investigations could be further strengthened. It will be annexed to the Commission's submission to the co-legislators as part of the evaluation process under Art. 19(1) of the OLAF Regulation and has been published on the Controller's website.[37]

In this opinion, the Controller emphasises the importance of ensuring greater clarity and effectiveness in the complaints mechanisms designed to safeguard fundamental rights and procedural guarantees during the investigative process. She also addresses the mandate and administrative status of the Controller, including considerations related to the functional independence of the role. In addition, she examines the complaints mechanism with a view to identifying potential avenues for improving accessibility, transparency, and procedural certainty for complainants. Finally, the opinion considers the institutional and operational relationships between the Controller and other key actors within the OLAF framework, including interactions with the OLAF Director-General, the Supervisory Committee, and other relevant stakeholders.

Most of the proposals set out in the opinion concern areas already discussed in this article. However, particular attention should be given below to those proposals with potentially more far-reaching impacts on the protection of the fundamental rights of persons concerned, the functioning of the complaints mechanism, and the function of the Controller, including relations with the OLAF Director-General.

The current OLAF Regulation distinguishes between the rights of persons concerned in internal and external investigations, resulting in differing levels of protection. In the Controller's view, however, the nature of an OLAF investigation (internal or external) should not, in principle, determine the

scope or intensity of the fundamental rights and procedural guarantees afforded to persons concerned. Therefore, as a general rule, the level of protection afforded to persons concerned should be aligned and equalised to the greatest extent possible across both types of investigations.[38]

As regards the rights of defence, particularly the right to be heard, the Controller also calls on the EU legislators to consider introducing clearer and more balanced rules in the OLAF Regulation regarding the information to be provided to persons concerned at the stage of the summary of facts. For the Controller, it is of the utmost importance that persons concerned are in a position to exercise their right to comment on the facts concerning them in a meaningful manner.[39] The Controller further proposes that the EU legislators consider extending the right to be heard so that persons concerned can submit observations not only on the facts established, but also on the provisional legal classification of those facts and on the preliminary conclusions drawn by OLAF.[40]

Another key proposal is to extend the personal scope of the complaints mechanism to include not only persons concerned but also witnesses, whistleblowers within the meaning of the Whistleblowing Directive,[41] informants under Art. 22a of the Staff Regulations,[42] other sources of information and victims of misconduct within OLAF's investigative remit.[43] In addition, the fundamental rights and procedural guarantees arising from such status should be provided for in the OLAF Regulation.[44] The opinion argues that the Controller was precisely established as an independent body entrusted with safeguarding procedural guarantees in the context of OLAF investigations, and thus should be given exclusive competence to examine all complaints relating to fundamental rights and procedural guarantees, irrespective of the complainant's status.

Regarding the function of the Controller in relation to the OLAF Director-General, the Controller proposes that the OLAF Regulation be amended to empower the Controller to issue opinions, addressed to the OLAF Director-General, on his or her own initiative, on any matter relating to fundamental rights, procedural guarantees, or the rules applicable to OLAF investigations that fall within the Controller's remit.[45]

V. Final Remarks

The first years of the function of OLAF's Controller of procedural guarantees have demonstrated that fundamental rights and procedural guarantees can be strengthened without compromising the effectiveness of OLAF investigations. As mentioned previously, my decisions have not only resolved individual complaints but also progressively shaped OLAF's investigative practice. This has been achieved by clarifying the scope and practical application of procedural guarantees and encouraging OLAF to better safeguard the rights of defence of persons concerned. As the complaints mechanism continues to evolve – in the words of the ECtHR: as a "living instrument" – its value will depend on sustained dialogue, transparency, and, where necessary, legislative refinement. It remains to be seen whether, and to what extent, the EU legislators will consider the recommendations issued by the Controller as part of the evaluation process of the OLAF Regulation (see above IV.). Regardless of the outcome of such legislative action, ensuring that fundamental rights and procedural guarantees remain operational, rather than merely declaratory, must remain a shared responsibility within the EU's anti-fraud architecture.

It is essential to raise greater awareness of the Controller's role and of the complaints mechanism available to those involved in OLAF investigations, in order to effectively protect their fundamental rights and procedural guarantees.[46] I hope that this article will draw the much-needed attention of legal practitioners and the wider legal community to the complaints mechanism and to the legal developments surrounding the function of the Controller.

*The author is the Controller of procedural guarantees as established by the reform of the OLAF Regulation. For reasons of neutrality, clarity, and generalisability, this article refers, as a rule, to "the Controller" in the third person and treats it as a function. The views expressed in this article are the author's personal views; confidentiality and data-protection obligations have been respected.

1 *D. Riochet* and *N. S. Mavromati,* "The Protection of Fundamental Rights and Procedural Guarantees in OLAF Investigations: a 25-Year Journey", (2024) eucrim, 316–323, p. 6 and footnote 44.

2 *Ibid.*, footnote 45.

3 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. See also *T. Wahl*, "OLAF's New Amended Legal Framework", (2020) eucrim, 276–277.

4 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

Prof. Dr. Julia Laffranque
Controller of procedural guarantees,
European Anti-Fraud Office (OLAF)

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.

5 Art. 2(5) of OLAF Regulation 883/2013.

6 R v Sussex Justices, Ex parte McCarthy, [1924] KB 256, [1923] All ER Rep 233.

7 Such rules include the new Guidelines on Investigation Procedures for OLAF Staff of 1 January 2026, available at: <https://anti-fraud.ec.europa.eu/document/download/e1994c22-7d58-4e61-8d34-0937a0be8f98_en?filename=gips-2026_en.pdf>; and the Guidelines on Digital Forensic Procedures for OLAF Staff of 11 February 2016, available at: <https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?filename=guidelines_en_bb84583638.pdf>. Note: All hyperlinks in this article were last accessed on 27 July 2026.

8 Cf. Recital 33 of Regulation 2020/2223 and Art. 9a(8) of the OLAF Regulation.

9 Cf. Art. 9a(8), sentence 2 and Art. 9b of the OLAF Regulation as amended by Regulation 2020/2223.

10 Charter of Fundamental Rights of the European Union, 2012/C 326/02, OJ C 326, 26.10.2012, 391–407.

11 Art. 52(3) of the Charter reads: "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention". Additionally, Art. 53 of the Charter provides that "[n]othing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised, in their respective fields of application, by […] international law and by international agreements to […] all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms […]." Furthermore, when applying EU law, the States Parties to the European Convention on Human Rights remain bound by the obligations they have voluntarily assumed when acceding to the Convention. *See* ECtHR [GC], 23 May 2016, *Avotiņš v. Latvia,* Appl. no. 17502/07, para. 101. These obligations must be assessed in the light of the presumption of equivalent protection established in ECtHR [GC], 30 June 2005, *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland,* Appl. no. 45036/98, ECHR 2005-VI.

12 *D. Riochet* and *N. S. Mavromati*, *op. cit.* (n. 1).

13 Art. 9b(6) of the OLAF Regulation as amended by Regulation 2020/2223.

14 Activity Report of the Controller of Procedural Guarantees for 2023, PUB/2024/863, OJ C, C/2024/5673, 23.9.2024, p. 5.

15 Art. 9b(3) of the OLAF Regulation and Arts. 11 and 12 of the Decision of the Controller of procedural guarantees adopting implementing provisions for the handling of complaints, 2022/C 494/07, PUB/2022/1609,OJ C 494, 28.12.2022, pp. 17–23, also available at: <https://supervisory-committee-olaf.europa.eu/controller-procedural-guarantees/about-controller/legal-framework_en>. For the latter, see also T. Wahl, "Controller of Procedural Guarantees Procedure of Handling Complaints", (2022) eucrim, 234.

16 *Ibid*.

17 Art. 228 TFEU and Regulation (EU, Euratom) 2021/1163 of the European Parliament of 24 June 2021 laying down the regulations and general conditions governing the performance of the Ombudsman's duties (Statute of the European Ombudsman) and repealing Decision 94/262/ECSC, EC, Euratom, OJ L 253, 16.7.2021, 1.

18 Art. 52 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC, PE/31/2018/REV/1, OJ L 295, 21.11.2018, 39 (the EU Data Protection Regulation), provides that the EDPS is responsible for monitoring and ensuring the application of this Regulation and of any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by an EU institution or body.

19 Under those rules, any person can lodge a complaint with the EDPS within 2 years of the date they became aware of the facts on which the complaint is based. See Art. 16(4), last indent, of the Decision of the European Data Protection Supervisor of 15 May 2020 adopting the Rules of Procedure of the EDPS, OJ L 204, 26.6.2020, 49.

20 Activity Report of the Controller of Procedural Guarantees for 2022, PUB/2023/803, OJ C 248, 13.7.2023, 1, subsection 3.3.2.; and Activity Report of the Controller of Procedural Guarantees for 2025, available at: <https://supervisory-committee-olaf.europa.eu/document/download/fa2f444e-3061-4710-991f-07e5389c30f8_en?filename=CTR%20Activity%20Report%202025_published.pdf>, subsection 4.1.2.

21 Activity Report of the Controller of Procedural Guarantees for 2022, *op. cit.* (n. 20), subsection 3.5.2.; Activity Report of the Controller of Procedural Guarantees for 2023, *op. cit.* (n. 14), subsection 4.2.; and Activity Report of the Controller of Procedural Guarantees for 2025, *op. cit.* (n. 20), section 4.3.

22 In the context of OLAF's process of revising its GIPs and based on Art. 9b(9) of the OLAF Regulation as amended by Regulation 2020/2223, the OLAF Director-General requested the opinion of the Controller on the newly revised text given the references and provisions contained therein on the procedural guarantees and fundamental rights that fall under Art. 9 of the OLAF Regulation and the Controller's mandate to ensure OLAF's compliance with them under the complaints mechanism (Art. 9b of the OLAF Regulation). The Controller submitted her opinion to the OLAF Director-General on 3 June 2024. A non-confidential version of the Controller's opinion is available here: <https://supervisory-committee-olaf.europa.eu/document/download/4f655d63-4b02-40df-8b93-038c44f1bb2e_en?filename=Opinion%20of%20the%20Controller%20on%20draft%20GIPs_redacted%20final.pdf>. Overall, the Controller welcomed the amendments introduced by OLAF in the GIPs following her remarks. She considered most of them implemented, either by means of the GIPs or though the Working Arrangements between OLAF and the Controller of Procedural Guarantees, which entered into force on 24 July 2025, available at: <https://supervisory-committee-olaf.europa.eu/document/download/ea81e700-4540-4ae6-b7ab-e56fb9a2d075_en?filename=SIGNED_WA_OLAF-Controller.pdf>.

23 For reference and comparison, see the original version of the GIPs and the newly adopted GIPs, valid as of 1 January 2026, both

available at: <https://anti-fraud.ec.europa.eu/guidelines-investigations-olaf-staff_en>.

24 Art. 9b(2) of the OLAF Regulation as amended by Regulation 2020/2223 provides: "Complaints shall be lodged within one month of the complainant becoming aware of the relevant facts that constitute an alleged infringement of the procedural guarantees or rules referred to in paragraph 1 of this Article. In any event, they shall be lodged no more than one month after the closure of the investigation. Complaints related to the notice period referred to in Article 9(2) and (4) shall, however, be lodged before the expiry of the 10-day notice period referred to in those provisions."

25 For a detailed account on the Controller's position on the one-month time limit for admissibility, *see* Activity Report of the Controller of Procedural Guarantees for 2022, *op. cit.* (n. 20), subsection 3.3.1; Activity Report of the Controller of Procedural Guarantees for 2023, *op. cit.* (n. 14), subsection 4.1; Activity Report of the Controller of Procedural Guarantees for 2024, PUB/2025/865, OJ C 4511, 7.8.2025, subsection 4.1; Activity Report of the Controller of Procedural Guarantees for 2025, *op. cit.* (n. 20), subsection 4.1.1; and Controller's Opinion on the evaluation of the application and impact of Regulation No. 883/2013, Ref. Ares(2026)2209882 – 27/02/2026, available at: <https://supervisory-committee-olaf.europa.eu/document/download/3c7a4446-920f-4cdb-92a3-f465e766a30e_en?filename=Annex%20-%20CTR%20Opinion%20on%20evaluation.pdf>, proposals 9 and 16.

26 Art. 37(5) of the GIPs.

27 Controller's Opinion on the evaluation of the application and impact of Regulation No. 883/2013, *op. cit.* (n. 25), proposals 4–5.

28 As explained under Art. 13 of the GIPs, "during the selection phase, the selection unit shall verify and analyse information of possible investigative interest and shall provide an opinion to the Director-General on whether an investigation or coordination case should be opened, or whether the case should be dismissed. The opinion shall also refer to whether the information should be reported to the EPPO or transferred to a competent authority of a Member State, or to an EU institution, body, office or agency."

29 Art. 5(1) of the OLAF Regulation.

30 Art. 21(2) of the GIPs.

31 Art. 12f(1) of the OLAF Regulation as amended by Regulation 2020/2223 provides that "[w]here the EPPO is conducting an investigation and the Director-General, in duly justified cases, considers that an investigation by the Office should also be opened in accordance with the mandate of the Office with a view to facilitating the adoption of precautionary measures or of financial, disciplinary or administrative action, the Office shall inform the EPPO in writing, specifying the nature and purpose of the investigation. […] In the event that the EPPO does not object within the time limit to be set in accordance with Article 12g, the Office may open an investigation, which it shall conduct in consultation with the EPPO on an ongoing basis."

32 Art. 8(1) and (2) of the Decision of the Controller of procedural guarantees adopting implementing provisions for the handling of complaints, op. cit. (n. 15).

33 Arts. 2(5) and 5(1) of the OLAF Regulation; and Art. 6 of former GIPs.

34 Art. 37(2) of the GIPs now requires that the registration in the OCM of an individual or legal person identified as person concerned in the opening decision be completed within one month. The clear deadline is intended to prevent delays that could adversely affect the right to be informed under Art. 9(3) of the OLAF Regulation, provided that this information does not prejudice the conduct of the investigation.

35 Art. 9(4) of the OLAF Regulation provides in its first indent that "[…] once the investigation has been completed and before conclusions referring by name to a person concerned are drawn up, that person shall be given the opportunity to comment on facts concerning him."

36 Art. 72(3) of the GIPs requires that the comments of persons concerned be summarised, assessed, and annexed to the final report, subject to the necessary safeguards concerning confidentiality, protection of procedural rights, and the conduct of other investigations.

37 Controller's Opinion on the evaluation of the application and impact of Regulation No. 883/2013, *op. cit.* (n. 25).

38 *Ibid.*, proposals 3–5.

39 *Ibid*., proposal 7.

40 *Ibid*., proposal 8.

41 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, OJ L 305, 26.11.2019, 17.

42 Regulation (EU, Euratom) No. 1023/2013 of the European Parliament and of the Council of 22 October 2013 amending the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union, OJ L 287, 29.10.2013, 15.

43 In the Dalli case, the Court of Justice of the EU held that OLAF's competence covers investigating allegations of serious misconduct and ethical breaches involving staff and members of institutions, bodies, offices and agencies of the EU. GC, 6 June 2019, Case T-399/17, Dalli v Commission, para. 62; upheld by the ECJ, 25 February 2021, Case C-615/19 P, Dalli v Commission. Therefore, OLAF's mandate extends beyond the protection of the Union's financial interests, including cases of sexual or psychological harassment.

44 Controller's Opinion on the evaluation of the application and impact of Regulation No. 883/2013, *op. cit.* (n. 25), proposals 11, 12, and 13.

45 Ibid., proposal 26.

46 All relevant information on how to lodge a complaint before the Controller can be found here: <https://supervisory-committee-olaf.europa.eu/controller-procedural-guarantees/submit-complaint_en>.

EU Procedural Rights Directives and their CJEU Evolution

Anže Erbežnik

The procedural rights of defendants in the EU have evolved through a combination of legislative harmonisation and judicial interpretation by the Court of Justice of the European Union (CJEU). Following the 2009 Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, key directives on the right to information, access to a lawyer, and the presumption of innocence established minimum standards to support the mutual recognition of judicial decisions in criminal matters. This article analyses how the CJEU has interpreted these instruments teleologically, thereby expanding, *inter alia*, their scope and the understanding of effective remedies while limiting derogations and preserving national procedural autonomy. Throughout this process, the CJEU has avoided EU rules on admissibility of evidence. The author argues that this development amounts to a "case law constitution" of EU criminal procedure, albeit one characterised by ongoing tensions. These notably concern the absence of common exclusionary rules of evidence and unresolved structural issues within the EU criminal justice system.

I. Introduction: Law as a Living Organism

As articulated by two great jurists in the past, law is in perpetual motion. *Oliver Wendell Holmes* observed that "[t]he life of the law has not been logic: it has been experience."[1] He went on to say that law is a product of history, moral and political theories, and the prejudices of judges and their era as "the rule adapts itself to the new reasons which have been found for it, and enters on a new career."[2] *Benjamin N. Cardozo* identified logic, history, custom, and morals as forces to which judges adhere.[3] He explained that the judge's role is not mechanical application but creative work.[4] Both jurists recognised that legal texts often contain gaps or ambiguities that require ongoing interpretation and adaptation to new developments. In Europe, this is reflected in the European Convention on Human Rights (ECHR) being considered a "living instrument," which means that the Convention must be interpreted in light of present-day conditions.[5] Such interpretation has enabled the European Court of Human Rights (ECtHR) to expand the scope of Convention rights beyond their original meaning. For example, Art. 6 ECHR has evolved to encompass the right to remain silent.[6] Art. 8 ECHR includes the protection of digital communications,[7] environmental quality,[8] and personal identity.[9]

The Court of Justice of the European Union (CJEU) operates under a similar philosophy, namely teleological interpretation.[10] Unlike strict textualism, the CJEU asks what objective a provision serves. Based on such logic, in the founding judgments *Van Gend en Loos* (1963)[11] and *Costa v. ENEL* (1964)[12], the Court transformed the Treaty of Rome from an international public law instrument into the constitutional foundation of a new legal order. In EU criminal law, this approach became evident in the Court's assessment of mutual trust as a basic principle of EU law,[13] and its assertion that EU law must be effective. In *Maria Pupino* (C-105/03),[14] the Court held that national courts must, as far as possible, interpret procedural law in conformity with framework decisions, even prior to the inclusion of the third pillar into the general EU legal order by the 2009 Lisbon Treaty. In *Melloni* (C-399/11),[15] it affirmed the primacy of EU law over national constitutional standards (e.g., judgments *in absentia*). And, more recently, in *G.K. and Others* (C-281/22),[16] the Court in Luxembourg resolved an ambiguity in the EPPO Regulation[17] regarding cross-border investigative measures. This teleological approach causes certain tensions in criminal law, however, given that criminal procedure is closely linked to national constitutional traditions, the organisation of the judiciary, and conceptions of justice.[18]

Before the Lisbon Treaty, an attempt to comprehensively harmonise defence rights at the EU level failed.[19] In its 2009 Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, the Council opted for a measure-by-measure approach under Art. 82(2) TFEU.[20] Six directives have been adopted so far (in chronological order): (1) on the rights on interpretation and translation;[21] (2) on information; (3) on access to a lawyer; (4) on the presumption of innocence; (5) on legal aid;[22] and (6) on procedural safeguards for children.[23] Together they constitute a system of rights that must be read alongside the minimum standard of the ECHR and the EU Charter of Fundamental Rights (in the following: the Charter), leaving significant interpretative space for the CJEU. It should also be borne in mind that these directives are the product of complex compromises. Hence, their text does not reflect the optimal legal solution, but rather what twenty-seven different political and legal traditions, along with the European

Parliament, could agree upon. Against this background, this article examines three of the six harmonising directives on defendants' rights ((2)–(4)), which have spawned extensive CJEU case law and interesting judicial interpretations.

II. Directive 2012/13/EU – The Right to Information

Directive 2012/13/EU[24] on the right to information in criminal proceedings is the EU's response to the US Miranda warnings, albeit broader in scope. It applies to all suspects, not just those in custody,[25] and covers warnings about the right to access a lawyer, free legal advice, the right to be informed of charges, the right to interpretation and translation, and the right to remain silent. For suspects not deprived of liberty, prompt oral or written notification is necessary. For arrested or detained persons, the Directive prescribes a written letter of rights, which must be accompanied by information on the maximum period before appearing before a judicial authority and the right to consular assistance. It also addresses the right to information about charges adapted to the different procedural stages. Furthermore, it establishes the right to access case materials, distinguishing between those essential for challenging detention (immediate access) and general evidentiary materials (access before trial). The Directive must be considered a *lex imperfecta,* however, as it does not regulate the admissibility or exclusion of evidence as a remedy in case of a violation of the right to information.[26] As will be shown in the following subsections, the CJEU provided several clarifications and added additional layers to the Directive regarding its scope, the modalities of the information provided, the nature of information to be provided, and the effective remedies.

1. Scope

The CJEU has interpreted the Directive broadly. In *Rayonna prokuratura Lom* (C-467/18), it extended the scope of the Directive (including that of Directive 2013/48) to judicial proceedings for the compulsory admission to a psychiatric institution for acts representing a danger. Such proceedings are closely linked to criminal accusations and may lead to deprivation of liberty.[27] The CJEU also clarified that national law cannot deny a national court the authority to verify respect for procedural rights during the earlier stages of pre-trial proceedings.[28] This is an important expansion of effective remedies and judicial control. Conversely, in *AB and Others* (C-203/20),[29] the Court held that the Directive does not apply to legislative procedures for revoking amnesties or constitutional reviews of them. This is an important reminder that, despite the CJEU's approach to read the scope of the Directive broadly, Directive 2012/13 is still tied to criminal proceedings.

In *Spetsializirana prokuratura* (C-649/19),[30] the Court distinguished between ordinary criminal proceedings and the execution of a European Arrest Warrant (EAW). It noted that Arts. 4, 6(2), and 7(1) of the Directive do not apply to EAW proceedings. This approach was reaffirmed in *IR*,[31] where the Court held that Arts. 6 and 47 of the Charter, the right to freedom of movement and residence, and the principles of equality and mutual trust do not oblige the judicial authority issuing an EAW to forward to the person sought the national arrest decision underlying the EAW or information on available legal remedies. These two judgments demonstrate that the Court has declined to extend the full scope of the Directive to the pre-surrender stage of the EAW system.

2. Information and service modalities

The first case requiring an interpretation of Directive 2012/13 by the CJEU was launched in 2014. A series of judgments in this context concerned the basic structure of the right to be informed, as well as the modalities of service of the information. In *Covaci* (C-216/14),[32] the CJEU ruled that non-resident accused persons must appoint an agent to accept service of a penalty order (*Strafbefehl*), provided that the accused enjoys the full period for lodging an objection (*Einspruch*). Thus, the Court tolerates procedural simplification, but only if it does not deprive the accused of the real opportunity to defence. In *Tranca and Others* (C-124/16, C-188/16 and C-213/16),[33] the Court confirmed that service on an authorised person is permissible provided that once the accused has actual knowledge of the penalty order, he or she is placed in the same position as if the order had been served personally, including through possible restoration to the *status quo ante*. This logic was reinforced in *Staatsanwaltschaft Offenburg* (C-615/18),[34] whereby Art. 6 of Directive 2012/13 precludes a subsequent criminal conviction based on non-compliance if the person concerned was unaware of the order (here: driving ban).

3. Accusation information and access to the file

Another group of cases concerned the timing and completeness of accusation information and access to the file. Regarding the linguistic dimension of the right to information, the CJEU reiterated in *IS* (C-564/19),[35] that Member States must take concrete measures to ensure the quality of interpretation and translation. This means that a person cannot be tried *in absentia* if he/she was not informed, in a language he/she understands, of the accusation due to inadequate interpretation. The same holds true if it is im-

possible to verify whether that information was effectively conveyed. In *Kolev and Others* (C-612/15),[36] the Court ruled that Art. 6(3) of Directive 2012/13 does not require to provide detailed information on the accusation before the case reaches the trial stage. This information can be provided after the indictment and even after the start of the hearing, provided that the rights of the defence and fairness of the proceedings are safeguarded. According to the Court, the same applies to Art. 7(3) of the Directive regarding access to the file. In this regard, a functional reading is preferred, which focuses on sufficient time and opportunity for defence. This issue arose again in *Kolev II* (C-704/18),[37] where the Court upheld national procedural autonomy and clarified that EU law does not oblige the trial court to remedy procedural defects, provided that the rights guaranteed by Arts. 6(3) and 7(3) of Directive 2012/13 were effectively protected. In *DS and KW [Stogenchev]* (C-342/25),[38] it also clarified that Art. 7(2) and (3) on access to case materials does not address admissibility of evidence or information in that regard.

Conversely, the CJEU held in *ZX* (C-282/20), that Art. 6(3), read together with Art. 47 of the Charter, applies throughout the criminal proceedings and precludes national legislation that does not provide for any procedural mechanism for remedying errors/omissions in an indictment that prejudice the accused's right to information about the charges after the pre-trial hearing.[39] It was also clarified that national courts must interpret national rules on amending charges in conformity with EU law as far as possible, in order to allow the prosecutor to remedy such defects while safeguarding defence rights actively and genuinely. This judgment is particularly important because it transforms the right to information into a procedural guarantee.[40] Another relevant issue is the distinction between factual changes and changes in legal classification. In *Moro* (C-646/17),[41] the Court held that Art. 6(4) of the Directive and Art. 48 of the Charter do not preclude national legislation under which an accused person may request a negotiated penalty during trial if the factual basis of the accusation changes. However, this is not permitted if only the legal classification changes. The decisive point was that the accused must be promptly informed of any such change to safeguard fairness and he/she must have an effective defence opportunity.

4. Effective remedy and the Charter

Ultimately, the CJEU dealt with issues involving the right to challenge failures to provide information. In *Politseyski organ pri 02 RU SDVR* (C-608/21),[42] it clarified that Art. 6(2) of the Directive does not require that all reasons for detention appear in the detention order, provided that the information supplied effectively enables the defence and is not provided only in the event that the legality of the detention is challenged. In *K.B. and F.S.* (C-660/21),[43] a structural gap in the Directive was addressed, as Art. 8 of Directive 2012/13 contains no express remedy for failures or refusals of the competent authorities to provide information in accordance with this Directive. This gap was filled by Arts. 47 and 48(2) of the Charter, as interpreted in the light of Arts. 6 and 13 ECHR. Hence, suspects must have a practical and effective opportunity to raise such a breach, including access to the file and a reasonable time to do so. This does not, however, automatically preclude national rules that prohibit courts from raising the issue on their own motion.

5. Interim conclusion

Overall, these judgments interpreting Directive 2012/13 show that the CJEU has transformed Directive 2012/13 into a comprehensive instrument for ensuring fairness in criminal proceedings. They feature the following crucial issues:

- Extending the scope of the Directive to areas that are not obviously covered, such as psychiatric committal proceedings;
- Insisting on practical and effective information, rather than formal notice;
- Tying information rights closely to access to the file, effective remedies, interpretation quality, and judicial review;
- Drawing limits in the specific context of the EAW and non-criminal procedures;
- Interpreting the Directive in dialogue with the Charter and ECtHR case law.

The result is a body of case law that is pragmatic in its refusal to impose automatic consequences, favouring contextual fairness instead.

III. Directive 2013/48/EU – The Right of Access to a Lawyer

Directive 2013/48/EU[44] is the most significant of the instruments envisaged in the 2009 Roadmap in terms of fair trial rights. It is also the most controversial piece, however, as it may have contributed to a lowering of ECtHR standards, whereby the ECtHR specifically referred to exceptions in its *Ibrahim and Others* judgment – foreseen in the Directive.[45] In this respect, ECtHR case law evolved from a clear affirmation of the right to a lawyer in pre-trial/police proceedings in the *Salduz* case,[46] to a right to a chosen lawyer in the *Dvorski* case,[47] and then back to a relativisation of the right to a lawyer in the aforementioned *Ibrahim case*. The Directive requires legal assistance in the following situations:

- Before questioning of suspects or accused persons by law enforcement authorities;

- Before investigative acts (e.g., identity parades, confrontations, and reconstructions);
- Without undue delay after deprivation of liberty; and
- Before the appearance of suspects/accused persons at a court with jurisdiction over criminal matters.

In terms of its substantial content, the Directive includes the following rights:

- The right to communicate confidentially with a lawyer before and during questioning;
- The right to communicate with third parties and consular authorities if a person is deprived of their liberty;
- The right to a lawyer in European Arrest Warrant proceedings, in both the executing and the issuing states.

Any waiver of the right must be voluntary and unequivocal, and it must be preceded by sufficient information. The Directive permits derogations in the pre-trial phase in exceptional circumstances, i.e., in cases of geographical remoteness and urgent necessity in order to avert serious adverse consequences for the person or the proceedings. However, attempts to introduce a more explicit EU admissibility/exclusionary rule in the event of a breach of the Directive's rights remained unsuccessful. Furthermore the Directive remains vague with regard to remedies as, for instance, it only refers to the need for having "effective remedies" in place and that, in the event of assessing statements from suspects/accused persons or of evidence obtained in breach of the rights, the national courts must merely take into account "respect of the rights of the defence and fairness of the proceedings."[48] As will be illustrated in the following subsections, the CJEU case law on Directive 2013/48 focused on the scope of the Directive underlining a broad understanding of proceedings covered, the waiver of such a right, possible derogations, the question of effective remedies, and applicability to vulnerable persons.

1. Scope

Similar to its case law on the Directive on information, the CJEU interpreted the scope of the Directive on the right to access a lawyer in broad terms. In *Rayonna prokuratura Lom*, the Court ruled that proceedings for compulsory psychiatric hospitalisation fell within the scope of the Directive, thus reinforcing the autonomous interpretation of the notion "criminal proceedings" (see also Section II.1 above).[49]

In *Rayonna prokuratura Lovech* (C-209/22), the CJEU clarified that Directives 2012/13 and 2013/48 apply from the moment a person is effectively treated as a suspect, even if national law does not recognise the concept of "suspect". Accordingly, for suspect status, two conditions must be fulfilled: (1) the existence of suspicion, and (2) information by official notification or otherwise.[50]

The Court ruled, however, that Member States are not required to introduce new remedies, and that limitations to judicial decision-making at the preliminary stage of criminal proceedings are acceptable, provided that, first, suspects can subsequently raise the issue before a court deciding on the substance of the case, and, secondly, that court can draw conclusions from an infringement, in particular as regards the inadmissibility or the probative value of the evidence.[51]

Ultimately, the CJEU clarified that the meaning of access to a lawyer "without undue delay" after deprivation of liberty (Art. 3(2)(c) of Directive 2013/48) does not necessarily mean "immediate" access, i.e. at the very moment of the deprivation of liberty. In the specific case of *Rayonna prokuratura Lovech,* this meant that a personal search and seizure at the preliminary stage of criminal proceedings did not automatically require access to a lawyer, provided that it was not necessary for the person to exercise defence practically and effectively.[52]

2. Validity of waiver

The CJEU has followed a strict approach as regards the conditions for a waiver of the right of access to a lawyer. In *Stachev* (C-15/24 PPU),[53] the Court ruled that a written waiver by an illiterate suspect is invalid if the consequences of waiving the right to a lawyer were not explained in a manner adapted to the suspect's vulnerability and the waiver was not recorded. This places positive obligations on law enforcement authorities. Furthermore, the Court clarified that the person concerned must be informed about the possibility to revoke the waiver before subsequent investigative acts take place.[54]

3. Derogations

Several CJEU judgments have addressed the possibility to derogate from the rights enshrined in the Directive. In *VW* (C-659/18), the Court ruled that the grounds for temporarily derogating from the right of access to a lawyer are listed exhaustively and must be interpreted narrowly. As a result, the failure of a suspect to appear following summons to appear before the investigative judge is not a ground for delaying access to a lawyer until the national arrest warrant issued against him/her has been executed. The CJEU made clear here that derogations cannot be extended by analogy or by reference to procedural convenience.[55] This approach confirms the Union legislators' intent to avoid scope creep

regarding derogations, as indicated in the Commission's implementation report.[56]

In its case law on the right to choose one's own lawyer, the CJEU aligns with the ECtHR decision in *Dvorski*.[57] However, it reaffirmed that this right is not absolute. In *Kolev and Others* (C-612/15),[58] the CJEU held that Art. 3(1) of Directive 2013/48 does not preclude national legislation allowing dismissal of the same lawyer acting for two accused persons if there is a conflict of interest. In *Stachev*, the Court followed up on its strict stance on derogations, stating that national police authorities cannot rely on Art. 3(6)(b), allowing temporary derogation where immediate action by the investigating authorities is imperative to prevent substantial jeopardy to criminal proceedings, if this provision has not been transposed into the national legal order.[59]

4. Remedial dimension and judicial review

As with other Roadmap directives, one of the main unresolved issues in Directive 2013/48 relates to remedies in the event of a violation. In the aforementioned case of *K.B. and F.S.* (see II.4. above),[60] the Court established the interconnection between a late notification of the right to remain silent and the access to a lawyer, if necessary having obtained legal aid. Further, examining the CJEU's case law on remedies for breaches of the rights to access a lawyer, the Court first applied a logic similar to that applied in its case law on the Directive on information: to preserve national procedural autonomy, but only on the condition that defence rights can be exercised effectively. This approach was evident, for example, in *DD* (C-347/21),[61] where an incriminating witness was examined in the absence of the accused and his/her lawyer for reasons beyond their control. According to the CJEU, the resulting breach may be remedied by an additional examination of this witness, provided that the accused and his/her lawyer receive the minutes of the questioning and are able to question the witness freely.

Similarly, in *Stachev*,[62] the Court held that Art. 12(2) of Directive 2013/48, read together with Art. 47 of the Charter, requires the court deciding on detention to be able to assess whether evidence was obtained in breach of access to a lawyer and, where appropriate, to disregard such evidence.

5. Vulnerable persons

Another crucial aspect of the Directive is ensuring access to a lawyer by vulnerable persons. The CJEU imposed positive duties on the authorities in this regard. In *Barało* (C-530/23),[63] it held that Member States are under an obligation to ensure that the vulnerability of a suspect is ascertained and acknowledged before they are questioned or investigative measures or measures of evidence gathering are carried out. The authorities must also ensure that such persons have access to a lawyer with the benefit of legal aid without undue delay and, at the latest, before questioning or before the relevant act is conducted. While the Court did not derive a formal presumption of vulnerability from EU law, it made clear that the authorities themselves must identify and address vulnerability in practice and that access to legal aid for vulnerable persons cannot depend on prior requests. In that regard, it was confirmed that Art. 12 of Directive 2013/48 (and Art. 8 of Directive 2016/1919) require for vulnerable persons reasoned decisions on their vulnerability, on refusal of legal aid, and on questioning without a lawyer, which must be open to challenge.[64]

6. Interim conclusion

The CJEU's case law on Directive 2013/48 has shown that the Court in Luxembourg has not simply replicated the Strasbourg Court's (ECtHR's) case law. Judgments such as *K.B. and F.S.*, *DD*, and *Kolev* demonstrate a willingness to tolerate certain procedural defects, delayed disclosure or delayed access, if these can be effectively raised or remedied at a later stage of the criminal proceedings and if the fairness of the proceedings as a whole is not compromised. Conversely, the judgments taken in *Stachev*, *Rayonna prokuratura Lom*, *VW*, *CH*, and *Barało,* for instance, demonstrate a potentially stricter approach than that taken by the ECtHR, particularly with regard to vulnerable persons and the availability of judicial review. Thus, we can conclude that the CJEU has not simply copied ECtHR case law, but rather follows a structured approach in which derogations must remain exceptional, vulnerability heightens the intensity of the need for protection on the part of the authorities, and effective remedies must exist in the national legal order. Procedural autonomy is only accepted insofar as it does not undermine the effectiveness of the rights guaranteed.

IV. Directive (EU) 2016/343 – The Presumption of Innocence

Directive (EU) 2016/343[65] addresses several aspects of the presumption of innocence, including:

- The prohibition on public portrayal of suspects as guilty;
- The prohibition on degrading presentations in court;
- The burden of proof; and
- The right to remain silent and the privilege against self-incrimination.

The Commission's original proposal would have permitted a reversed burden of proof in certain circumstances, and

the Council wanted silence to be a relative right capable of negative consequences, in line with the ECtHR's ruling in *John Murray v. United Kingdom*.[66] However, the European Parliament successfully campaigned for the right to remain silent to be enshrined as an absolute right. As a compromise, the question of the legal remedy and exclusionary rules of evidence is left to the "effective remedy" formula that runs throughout all the Roadmap directives. Looking at Directive 2016/343 at a glance, it can be noted that it sets high standards regarding the presumption of innocence, but only mediocre standards regarding the right to be present at trial and its derogations establishing no obligatory retrial.[67] In the latter regard, the Directive largely follows the provisions of Framework Decision 2009/299/JHA.[68] Regarding Directive 2016/343, the CJEU has focused primarily on its scope, public references to guilt, the right to be present at trials, and judicial independence – the case law of which is outlined in the following subsections.

1. Scope

As with the Directives on information and access to a lawyer, the CJEU had to clarify the scope of Directive 2016/343. In *Emil Milev* (C-310/18 PPU),[69] the Court interpreted Arts. 3 and 4(1), ruling that preliminary procedural decisions, including pre-trial detention, can be based on suspicion/incriminating evidence, provided that the decision does not characterise the person as guilty. This approach was reinforced in *DK* (C-653/19 PPU),[70] where the Court held that Art. 6 of the Directive on the burden of proof does not apply to national rules making release from pre-trial detention conditional upon the accused demonstrating changed circumstances. As mentioned above, the CJEU extended the reach of the Directive beyond ordinary criminal trials in *Rayonna prokuratura Lom,* such that the Directive also covers compulsory psychiatric committal.[71]

2. Public references to guilt

Art. 4 of the Directive, which regulates the presumption of innocence in the context of public references to guilt, was in the spotlight in case *AH and Others* (C-377/18).[72] Here, the CJEU ruled that a plea agreement procedure, in which only one of the co-accused pleaded guilty while mentioning others, is compatible with Art. 4(1). However, this is only permitted if such a reference is necessary for the characterisation of the legal liability of the person who entered into the agreement and if the agreement makes it clear that the guilt of the other co-accused has not yet been legally established.

Further, in case *AC [Kotaňák]* (C-748/24),[73] it ruled that regarding Arts. 3, 4(1) and 6(1) of Directive 2016/343, an appellate court may examine the evidence in detail and assess whether the legal elements of the alleged offence are met when reviewing a decision to close criminal proceedings because no offence was committed. This is permitted even if national law does not require such an assessment and even if the court relies solely on evidence collected during the investigation, without the accused having had a chance to comment on that evidence. However, the presumption of innocence prohibits the court from adopting reasoning that expresses or implies a view that the accused is guilty of the criminal offence in question. Whether this threshold has been crossed depends on the wording of the decision, read in its full particular context and in light of the nature and stage of the proceedings.

3. Presence at trial

A significant amount of case law refers to the right to be present at trial, which forms part of the major dimensions of Directive 2016/343; it is regulated in Arts. 8 and 9. In *TX and UW* (C-688/18),[74] the CJEU held that Art. 8(1) and (2) is not infringed if an accused person, who has been duly informed and represented by a lawyer, decides unequivocally not to attend one of the hearings. The same applies if the person was absent for reasons beyond his or her control, provided that, once informed, he or she either waives his/her right to object or is given the possibility of having the steps taken in his absence repeated effectively. The Court underlines here that Art. 8 protects effective participation, not mere physical presence. This concept was further refined in *DD*,[75] where the Court held that, if a witness had been examined in the absence of the accused or his/her defence lawyer for reasons beyond their control, the violation of the right to be present can be remedied by an additional examination at which the accused and lawyer can question the witness. Full repetition of the earlier examination is not required.

In *HYA and Others* (C-348/21),[76] the Court moved beyond the two aforementioned rulings holding that a conviction cannot be based on witness testimony taken before a judge at the pre-trial stage, without the participation of the accused or his/her lawyer, unless there was a good reason for the witness's absence at trial, the testimony was not the sole or decisive basis for the conviction, and sufficient counterbalancing safeguards existed. This judgment marks a shift from a restrained approach, as Art. 8 was interpreted in close conjunction with the broader fair-trial guarantees of the Charter and ECtHR case law. In *HN* (C-420/20),[77] the CJEU held that Art. 8(1) does not preclude national legislation that makes the presence of the accused at trial mandatory. However, Art. 8(2) prevents a Member State from holding a trial *in absentia* if the accused is outside the coun-

try and cannot lawfully re-enter because of an entry ban imposed by that same State. Hence, the person must have a genuine opportunity to attend, or voluntarily and unequivocally waive that option.[78]

4. *In absentia* trials

The other side of the coin of the right to be present at trial is the question of whether Member States can hold trials in the absence of the defendant. The first major judgment to interpret Arts. 8 and 9 of Directive 2016/343 concerning absconded defendants tried *in absentia* was *IR* (C-569/20).[79] The CJEU ruled that a new trial or an equivalent remedy can only be denied if precise and objective indicia show that the person had sufficient information to know that a trial would take place and deliberately avoided the official notice with the intention of evading justice.

That same line of argumentation was applied in *TR* (C-416/20 PPU),[80] this time in the context of the EAW. According to the CJEU, the executing authority may not refuse surrender merely because it lacks assurance that the convicted person will enjoy the right to a new trial after surrender. The ruling confirms that Directive 2016/343 does not add refusal grounds to Framework Decision 2002/584/JHA on the EAW, even though the issuing State is still required to comply with the Directive.

A refined approach was taken in *Stangalov* (C-644/23),[81] where the CJEU denied a new trial to a person who absconded after receiving a preliminary indictment during the pre-trial stage if, in the light of all the circumstances, the person may be regarded as having been informed of the trial and was either represented by a mandated lawyer or, in the absence of such representation, had been informed in due time of the consequences of absconding. Thus, absconding alone does not extinguish the right to a new trial. In *Kachev* (C-135/25 PPU),[82] the CJEU clarified in view of Art. 8(2)(a) and (b) of the Directive that authorities must have made reasonable efforts to locate the person in question and have actually delivered the trial details to the address provided, after the person received a corresponding preliminary indictment; they must also have ensured genuine legal representation (e.g., court-appointed counsel during the pre-trial stage is not sufficient).

The CJEU also clarified the remedial approach in *VB* (C-430/22 and C-468/22),[83] holding that Art. 8(4) does not require the national trial court to indicate the right to a new trial in the *in absentia* judgment; the Directive only requires that the person be informed of that right when he/she is informed of the decision rendered *in absentia*. In *VB II* (C-400/23),[84] however, the Court stated that requests for a new trial must be examined promptly, and that upon notification of the decision, the defendant must receive a full copy of the decision rendered *in absentia* together with clear and understandable information on the available remedies and procedure. It was also confirmed that the existence of the right to a new trial depends exclusively on whether the conditions of Art. 8(2) of Directive 2016/343 are met, leaving no room for discretion in this regard.[85]

In recent decisions, the CJEU has had to deal with modern forms of participation. In *FP and Others* (C-760/22),[86] it held that Art. 8(1) does not prevent an accused person from participating in hearings via videoconference at his/her express request, provided that the right to a fair trial is upheld. The CJEU also clarified *in CV [Casotta]* (C-24/26 PPU)[87] that higher national standards are permissible provided they do not undermine the primacy, unity, or effectiveness of EU law. Accordingly, national legislation may require direct proof that the accused deliberately avoided the proceedings, before refusing a retrial to a person convicted *in absentia*.

5. Reclassification and judicial independence as dimensions of the presumption of innocence

The issue of reclassifying the offence is relevant not only for the right to information but also in the context of the presumption of innocence. This connection became apparent in *BK* (C-175/22).[88] The CJEU held that, under Art. 6(4) of Directive 2012/13, a criminal court cannot reclassify an offence in its judgment without first informing the accused in due time and giving him an opportunity to effectively defend himself against the new classification. In parallel, the Court, however held that neither the presumption of innocence under Art. 3 nor the privilege against self-incrimination under Art. 7 of Directive 2016/343, nor Art.47 of the Charter, prevent the national court from proposing or adopting a different legal classification, even on its own initiative, provided the accused is properly informed and heard. This case clarifies that judicial initiative in classification does not in itself violate the presumption of innocence; what matters is the preservation of defence rights and procedural fairness.

Finally, in *WB and Others* (C-748/19 to C-754/19), the Court addressed the presumption of innocence in the broader institutional context of judicial independence. It ruled that national provisions allowing the Minister of Justice to second judges to higher courts on the basis of unpublished criteria, and to revoke those secondments at any time without reasons, are incompatible with the second subparagraph of Art. 19(1) TEU, read in the light of Art. 2 TEU, and with Art. 6(1) and (2) of Directive 2016/343.[89]

6. Interim conclusion

Overall, the line of case law on Directive 2016/343 demonstrates gradual but distinct development in the CJEU's understanding of the rights enshrined in the Directive. The early judgments, particularly *Milev* and *DK*, emphasised limitations and confined the Directive to preventing premature expressions of guilt. Subsequent judgments have mostly focused on the right to be present at trial. In this context, the CJEU affirmed the protection of effective participation rather than formal attendance. For convictions *in absentia* either genuine notice and waiver, or a robust right to a fresh determination of the merits are required.

V. Conclusion: A Caselaw Constitution of EU Criminal Procedure

The procedural rights directives following the 2009 Council Roadmap and the ensuing CJEU case law that has developed alongside them are a notable achievement, albeit an imperfect one. Like *Holmes'* and *Cardozo's* narratives, outlined in the introductory remarks of this article, the CJEU has used the directives as building blocks in the broader constitutional framework of "EU fair trial". Predominantly teleological interpretation has been employed to ensure that rights are real and effective, not merely on paper.

Several conclusions can be drawn from the case law analysed in this article. Firstly, the CJEU interprets the autonomous concept of "criminal proceedings" broadly in order to bring them within the scope of the Directives. Secondly, the Court has repeatedly reinforced the obligation for Member States to provide effective remedies; it conferred upon national courts the procedural power to verify compliance with the Directives, even where national procedural law might preclude such review. Thirdly, the Court in Luxembourg has generally interpreted derogations from fundamental rights narrowly. Fourthly, the Court has used the Directives as a framework through which it enforces its own vision of the EU criminal law area, which is based on mutual trust and the rule of law.

Despite these positive features, three systemic tensions persist. Firstly, there is a risk of a negative feedback loop between EU harmonisation and ECtHR case law, as above indicated by *Ibrahim and Others* on derogations from the right to a lawyer. EU procedural rights Directives that codify derogations may prompt the ECtHR to narrow the standards of the European Convention on Human Rights. In *Ibrahim and Others*, the ECtHR re-interpreted its ruling in the *Salduz* case by referring, *inter alia*, to Directive 2013/48. The issue of trials *in absentia* is another example where a real danger of divergence between the system of the EU and that of the Council of Europe exist. Secondly, the analysis demonstrated the lack of proper common admissibility/exclusionary rules in the EU legal framework. None of the procedural rights Directives adopted until today contain a clear rule on the admissibility of evidence in case of violations of the rights enshrined. The prevailing formula that "the rights of defence must be respected and the overall fairness of proceedings be ensured" is a method of judicial weighing rather than a clear normative standard. The formula instead reinforces divergent and unequal results across EU Member States.[90] Thirdly, there is the "EPPO paradox", meaning that we presume the existence of a substantially harmonised area of criminal procedure by creating supranational bodies (e.g., the EPPO) that lack a real supranational code of criminal procedure.

The creation of a European area of criminal justice, in which defendants across the EU enjoy effective, real, and equivalent procedural protection at a high level, remains a work in progress. Key issues in this context are that some procedural rights Directives provide exceptions (e.g., Directive 2013/48 on the right of access to a lawyer), thus allowing for different interpretation and standards, that the issue of admissibility of evidence in case of violations of rights guaranteed has not been clearly addressed, and that investigative measures and their authorisation remain significantly divergent between EU Member States (e.g., measures on secret surveillance).[91] Only once these issues have been addressed and "checkerboard situations"[92] avoided, we will be able to speak of a genuine area of European criminal justice. This article demonstrated that the CJEU is contributing to this through its evolutionary approach to law; it slowly advances the acquis towards a more far-reaching destination through incremental steps.

---

* The opinions expressed in this article are those of the author and cannot be attributed to the institution which employs him.

1 O.W. Holmes, Common *Law*, 1881, p. 1.

2 Holmes, *op. cit.* (n. 1), p. 5.

3 B. N. Cardozo, *The Nature of the Judicial Process*, 2021, pp. 30–31.

4 Cardozo, *op. cit.* (n. 3), pp. 14 and 115.

5 ECtHR, 25 April 1978, *Tyrer v. United Kingdom,* Appl. no. 5856/72, para. 31.

6 ECtHR, 25 February 1993, *Funke v. France*, Appl. no. 10828/84, para. 44; ECtHR, 17 December 1996, *Saunders v. United Kingdom,* Appl. no. 19187/91, para. 68.

7 ECtHR, 1 July 2008, *Liberty and Others v. United Kingdom*, Appl. no. 58243/00, para. 56.

8 ECtHR [GC], 9 April 2024, *Verein Klimaseniorinnen Schweiz and Others v. Switzerland*, Appl. no. 53600/20, para. 573.

Prof. Dr. Anže Erbežnik, Berkeley Law, LLM
Legal Affairs Committee, European Parliament, Administrator

9 ECtHR [GC], 11 July 2002, Appl. no. 28957/95, *Christine Goodwin v. United Kingdom*, para. 75.
10 See G. Conway, *The Limits of Legal Reasoning and the European Court of Justice*, 2012.
11 CJEU, 5 February 1963, Case 26/62, *van Gend en Loos* [ECLI:EU:C:1963:1].
12 CJEU, 15 July 1964, Case 6/64, *Costa v. ENEL* [ECLI:EU:C:1964:66].
13 CJEU, 18 December 2014, Opinion 2/13 [ECLI:EU:C:2014:2454], para. 191.
14 CJEU, 16 June 2005, Case C-105/03, *Maria Pupino* [ECLI:EU:C:2005:386], para. 43.
15 CJEU, 26 February 2013, Case C-399/11, *Stefano Melloni* [ECLI:EU:C:2013:107], para. 63.
16 CJEU, 21 December 2023, Case C-281/22, *G.K. and Others* [ECLI:EU:C:2023:1018], para. 78.
17 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, OJ L 283, 31.10.2017, p. 1.
18 A. Erbežnik, "The Principle of Mutual Recognition as a Utilitarian Solution, and the Way Forward," (2012) 2(1) *European Criminal Law Review (EuCLR)*, 3–19.
19 Proposal for a Council framework Decision on certain procedural rights in criminal proceedings throughout the European Union, COM(2004) 328 final.
20 Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, OJ C 295, 4.12.2009, 1.
21 Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, OJ L 280, 26.10.2010, 1. For this Directive, see S. Cras and L. De Matteis, "The Directive on Interpretation and Translation in Criminal Proceedings", (2010) *eucrim*, 153–162; M. Kotzurek, "Directive 2010/64/EU on translation and interpretation services in criminal proceedings: A new quality seal or a missed opportunity?", <https://doi.org/10.30709/eucrim-2021-034> accessed 4 August 2026.
22 Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, 1. For this Directive, see S. Cras, "The Directive on the Right to Legal Aid in Criminal and EAW Proceedings", (2017) *eucrim*, 34–45; B. Vidal Fernández, "Implementation of the Legal Aid Directive in Spain", (2020) *eucrim*, 55–59.
23 Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 1.5.2016, 1. For this Directive, see S. Cras, The Directive on Procedural Safeguards for Children who Are Suspects or Accused Persons in Criminal Proceedings", (2016) *eucrim*, 109–119.
24 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, 1.
25 US Supreme Court, 13 June 1966, *Miranda v. Arizona*, 384 U.S. 436; see also US Supreme Court, 5 May 1976, *Beckwith v. United States*, 425 U.S. 341, regarding the limitation of the Miranda warning to custodial settings.
26 S. Cras and L. De Matteis, "The Directive on the Right to Information, Genesis and Short Description," (2013) *eucrim*, 22–32; A. Pivaty and A. Soo, "Access to the Case Materials in Pre-Trial Stages", (2019) *eucrim*, 60–65.
27 CJEU, 19 September 2019, Case C-467/18, *EP (Rayonna prokuratura Lom)* [ECLI:EU:C:2019:765], paras. 42–45.
28 CJEU, *EP (Rayonna prokuratura Lom), op. cit.* (n. 27), paras. 55–63.
29 CJEU, 16 December 2021, Case C-203/20, *AB and Others* [ECLI:EU:C:2021:1016], para. 72.
30 CJEU, 28 January 2021, Case C-649/19, *IR (Spetsializirana prokuratura)* [ECLI:EU:C:2021:75], para. 62.
31 CJEU, 30 June 2022, Case C-105/21, *IR* [ECLI:EU:C:2022:511], paras. 59–60.
32 CJEU, 15 October 2015, Case C-216/14, *Covaci* [ECLI:EU:C:2015:686], para. 68.
33 CJEU, 22 March 2017, Joined Cases C-124/16, C-188/16 and C-213/16, *Tranca and Others* [ECLI:EU:C:2017:228], paras. 50–51.
34 CJEU, 14 May 2020, Case C-615/18, *UY (Staatsanwaltschaft Offenburg)* [ECLI:EU:C:2020:376], para. 63.
35 CJEU, 23 November 2021, Case C-564/19, *IS* [ECLI:EU:C:2021:949], para. 138.
36 CJEU, 5 June 2018, Case C-612/15, *Kolev and Others* [ECLI:EU:C:2018:392], paras. 99–100.
37 CJEU, 12 February 2020, Case C-704/18, *Kolev and Others II* [ECLI:EU:C:2020:92], para. 57.
38 CJEU, 11 June 2026, Case C-342/25, *DS and KW [Stogenchev]* [ECLI:EU:C:2026:469], paras. 50–54.
39 CJEU, 21 October 2021, Case C-282/20, *ZX* [ECLI:EU:C:2021:874], para. 32.
40 CJEU, *ZX, op. cit.* (n. 39), para. 45.
41 CJEU, 13 June 2019, Case C-646/17, *Moro* [ECLI:EU:C:2019:489], para. 74.
42 CJEU, 25 May 2023, Case C-608/21, *XN (Politseyski organ pri 02 RU SDVR)* [ECLI:EU:C:2023:426], paras. 58 and 76.
43 CJEU, 22 June 2023, Case C-660/21, *K.B and F.S.* [ECLI:EU:C:2023:498], paras. 40–41.
44 Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, 1.
45 ECtHR [GC], 13 September 2016, Appl. nos. 50541/08, 50571/08, 50573/08 and 40351/09, *Ibrahim and Others v. United Kingdom*, para. 259.
46 ECtHR [GC], 27 November 2008, Appl. no. 36391/02, *Salduz v. Turkey*, para. 55.
47 ECtHR [GC], 20 October 2015, Appl. no. 25703/11, *Dvorski v. Croatia*, paras. 100–102.
48 S. Cras, "The Directive on the right of access to a lawyer in criminal proceedings and in European arrest war-rant proceedings," (2014) *eucrim*, 32–44; A. Soo, "(Effective) Remedies for a Violation of the Right to Counsel during Criminal Proceedings in the European Union: An Empirical Study," (2018) 14(1) *Utrecht Law Review*, 18–60; A. Soo, "How are the member states progressing on transposition of Directive 2013/48/EU on the right of access to a lawyer?: An inquiry conducted among the member states with the special focus on how Article 12 is transposed", (2017) 8(1) *New Journal of European Criminal Law (NJECL)*, 64–76.

49 CJEU, *EP (Rayonna prokuratura Lom*), *op. cit.* (n. 27), para. 54.
50 CJEU, 7 September 2023, Case C-209/22, *AB (Rayonna prokuratura Lovech*) [ECLI:EU:C:2023:634], paras. 33–45, in particular para. 39.
51 CJEU, *AB, op. cit.* (n. 50), paras. 46–61.
52 CJEU, *AB, op. cit.* (n. 50), paras. 73–78.
53 CJEU, 14 May 2024, Case C-15/24 PPU, *CH (Stachev)* [ECLI:EU:C:2024:399], para. 54–70.
54 CJEU, *CH, op. cit.* (n. 53), para. 80.
55 CJEU, 12 March 2020, Case C-659/18, *VW* [ECLI:EU:C:2020:201], paras. 43–48.
56 European Commission, Report on the implementation of Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third person informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (COM/2019/560 final).
57 ECtHR [GC], *Dvorski v. Croatia*, *op. cit.* (n. 47), paras. 103–113.
58 CJEU, *Kolev and Others*, *op. cit.* (n. 36), para. 111.
59 CJEU, *CH, op. cit.* (n. 53), paras. 46–53.
60 CJEU, *K.B and F.S., op. cit.* (n. 43), para. 53.
61 CJEU, 15 September 2022, Case C-347/21, *DD* [ECLI:EU:C:2022:692], para. 46.
62 CJEU, *CH, op. cit.* (n. 53), para. 99.
63 CJEU, 8 May 2025, Case C-530/23, *K.P. (Barało)* [ECLI:EU:C:2025:322], para. 92.
64 CJEU, *K.P., op. cit.* (n. 63), para. 108.
65 Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1.
66 ECtHR [GC], 8 February 1996, Appl. no. 18731/91, *John Murray v. United Kingdom*, para. 47.
67 S. Cras and A. Erbežnik, "The Directive on the Presumption of Innocence and the Right to Be Present at Trial, Genesis and description of the new EU-Measure," (2016) *eucrim*, 25–36; A. Pivaty *et al.* , "Opening Pandora's box: The right to silence in police interrogations and the Directive 2016/343/EU," (2021) 12(3) *New Journal of European Criminal Law (NJECL)*, 328–346; see also European Commission, Report on the implementation of Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, COM/2021/144 final.
68 Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial, OJ L 81, 27.3.2009, 24.
69 CJEU, 19 September 2018, Case C-310/18 PPU, *Emil Milev* [ECLI:EU:C:2018:732], para. 49.
70 CJEU, 28 November 2019, Case C-653/19 PPU, *DK (Spetsializirana prokuratura)* [ECLI:EU:C:2019:1024], para. 42.
71 CJEU, *EP, op. cit.* (n. 27), paras. 54, 68. However, the Directive does not apply to purely therapeutic psychiatric committal proceedings.
72 CJEU, 5 September 2019, Case C-377/18, *AH and Others* [ECLI:EU:C:2019:670], para. 50.
73 CJEU, 30 April 2026, Case C-748/24, *AC (Kotaňák)* [ECLI:EU:C:2026:358], paras. 61–80.
74 CJEU, 13 February 2020, Case C-688/18, *TX and UW* [ECLI:EU:C:2020:94], para. 49.
75 CJEU, *DD, op. cit.* (n. 61), para. 46.
76 CJEU, 8 December 2022, Case C-348/21, *HYA and Others* [ECLI:EU:C:2022:965], para. 62.
77 CJEU, 15 September 2022, Case C-420/20, *HN* [ECLI:EU:C:2022:679], paras. 43 and 66.
78 CJEU, *HN, op. cit.* (n. 77), paras. 51–58. See also CJEU, 21 May 2026, Case C95/24, *ATAU (Khuzdar)* [ECLI:EU:C:2026:416], paras. 67–69, and CJEU, 21 May 2026, Case C-447/24, *SO (Höldermann)*, [ECLI:EU:C:2026:417], paras. 75–77, regarding the same interpretation of Framework Decision 2008/909.
79 CJEU, 19 May 2022, Case C-569/20, *IR* [ECLI:EU:C:2022:401], para. 59.
80 CJEU, 17 December 2020, Case C-416/20 PPU, *TR (Generalstaatsanwaltschaft Hamburg)* [ECLI:EU:C:2020:1042], para. 56.
81 CJEU, 16 January 2025, Case C-644/23, *IR (Stangalov)* [ECLI:EU:C:2025:16], para. 52. See also T. Wahl, "ECJ Ruled on Right to New Trial if Suspect Absconds", *eucrim* 4/2024, 288–289.
82 CJEU, 20 May 2025, Case C-135/25 PPU, *M.S.T. (Kachev)* [ECLI:EU:C:2025:366], para. 71.
83 CJEU, 8 June 2023, Joined Cases C-430/22 and C-468/22, *VB and VB* [ECLI:EU:C:2023:458], para.31.
84 CJEU, 16 January 2025, Case C-400/23, *VB II* [ECLI:EU:C:2025:14], para. 75.
85 For an analysis of this ruling, see J. Callewaert, "A Different Understanding of the Waiver of the Right to Attend Trial – Judgment of the CJEU in the Case of VB II", <https://johan-callewaert.eu/a-different-understanding-of-the-waiver-of-the-right-to-attend-trial-judgment-of-the-cjeu-in-the-case-of-vb-ii/> (accessed 4 August 2026), who submits that the judgment in *VB II* transforms the right to a new trial into a procedural consequence of non-compliance with the conditions set out in Art. 8(2), rather than a safeguard linked to the ECtHR's case law focusing on the fairness of the proceedings, and thus reinforces the objectivised, condition-based structure of the Directive. See also T. Wahl, "ECJ Rules on Conditions for in absentia Judgments", *eucrim* 4/2024, 287–288.
86 CJEU, 4 July 2024, Case C-760/22, *FP and Others* [ECLI:EU:C:2024:574], para. 32.
87 CJEU, 23 April 2026, Case C-24/26 PPU, *CV [Casotta]* [ECLI:EU:C:2026:333], paras.114–118.
88 CJEU, 9 November 2023, Case C-175/22, *BK* [ECLI:EU:C:2023:844], paras. 55–61.
89 CJEU, 16 November 2021, Joined Cases C-748/19 to C-754/19, *WB and Others* [ECLI:EU:C:2021:931], para. 90.
90 See. European Law Institute, "Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings", <https://www.europeanlawinstitute.eu/projects-instruments/instruments/eli-proposal-for-a-directive-of-the-european-parliament-and-the-council-on-mutual-admissibility-of-evidence-and-electronic-evidence-in-criminal-proceedings/> (accessed 4 August 2026), which tried to establish such rules by an academic proposal. For the proposal, see also L. Bachmaier, "Mutual Admissibility of Evidence and Electronic Evidence in the EU – A New Try for European Minimum Rules in Criminal Proceedings?", (2023) *eucrim*, 223–229.
91 In that regard, the Commission is trying to achieve a certain level of harmonisation through cross-border rules, as set out in the recent proposed changes to cross-border surveillance measures foreseen in the proposed amendments to Directive 2014/41 regarding the European Investigation Order: Proposal for a Directive of the European Parliament and the Council regarding the European Investigation Order in criminal matters and the European Remote Participation Order (recast), COM(2026) 313 final, e.g., Arts. 30, 33 and 34.
92 Dworking used the term "checkerboard laws" to describe situations where inside the same legal area contradictory perceptions exist. R. Dworkin, *Law's Empire*, Harvard University Press, 2001, pp. 179–186. See also A. Erbežnik, (2012) 2(1) *EuCLR*, *op. cit.* (n. 18).

Reinforcing EU Core Values in Criminal Justice

Insights from the High-Level Forum on the Future of EU Criminal Justice

Katalin Ligeti

This article reflects on the future direction of EU criminal policy in light of the discussions held at the High-Level Forum on the Future of EU Criminal Justice (HLF). It proceeds from the premise that EU criminal law forms an integral part of the broader EU acquis and is grounded in a set of shared foundational values. The author therefore argues that future EU criminal policy should place the protection and promotion of the values enshrined in Article 2 of the Treaty on European Union – including the rule of law, fundamental rights, and democracy – at the centre of its development. Drawing on selected examples from both substantive and procedural criminal law, the author identifies areas in which a renewed emphasis on these values is particularly important for shaping future EU legislation. In conclusion, the article assesses the prospects for this approach in light of the outcomes of the High-Level Forum and considers its implications for the future development of EU criminal law.

I. Introduction

In 2025, the European Commission launched a High-Level Forum for the Future of European Criminal Law[1] (HLF), which brought together representatives of EU Member States, EU criminal justice agencies and bodies, professional organisations from various branches of criminal law practice, and academia. The aim of the HLF was to revive the tradition of comprehensive EU criminal policy programmes — such as the Tampere Programme,[2] the Hague Programme,[3] and the Stockholm Programme[4] — through which both Member States and EU institutions would jointly articulate a vision for the development of the Area of Freedom, Security and Justice over the following five-year period.

Following the entry into force of the Lisbon Treaty, Art. 68 of the Treaty on the Functioning of the European Union (TFEU) entrusted the European Council with the task of defining strategic guidelines for legislative and operational planning within the AFSJ. As a consequence, the above-mentioned ambitious, multiannual programmes that had previously structured the development of EU criminal policy were replaced by more general strategic guidelines adopted by the European Council. This evolution can be explained, at least in part, by the institutional changes brought about by the Lisbon Treaty. In particular, the Treaty substantially strengthened the role of the European Commission in the field of criminal justice by extending the application of the ordinary legislative procedure and by consolidating the Commission's right of legislative initiative regarding the approximation of substantive and procedural criminal law under Arts. 82 and 83 TFEU.

Since 2009, the Union has actively exercised these enhanced competencies, adopting a wide range of legislative initiatives across the criminal law domains envisaged by the Lisbon Treaty.[5] Against this background, the Commission considered the time ripe to take stock of the developments that had occurred since the Treaty's entry into force and to reflect on the future direction of EU criminal policy. The HLF was conceived as a forum for such reflection, bringing together European criminal law experts to discuss both the achievements of the past decade and the challenges likely to shape the next phase of European criminal justice integration. The discussion was structured around thematic blocs like substantive criminal law, procedural criminal law and judicial cooperation, procedural safeguards in criminal proceedings, the digitalisation of criminal justice, and EU JHA agencies and bodies.

This article contributes to this analysis, building on the author's statement at the opening of the HLF. It is based on the premise that the AFSJ forms an integral part of the broader EU *acquis*, which is rooted in shared core values.[6] Therefore, future EU criminal policy should prioritise safeguarding and promoting the core values enshrined in Art. 2 of the Treaty on European Union (TEU), including the rule of law, fundamental rights, and democracy. To this end, the article first provides a concise historical overview of the role and significance of these core values in shaping EU criminal law to date. It then refers to key examples of substantive and procedural criminal law where renewed emphasis on these values is particularly necessary to shape future EU legislation. The article concludes by assessing the prospects for a value-driven approach to the future development of EU criminal law, based on the outcomes of the HLF.

II. Core Values of Criminal Justice as a Starting Point for Developing a Five-Year Vision

Today, EU criminal law is an established part of the EU *acquis*. Its emergence, however, was by no means self-evident. In fact, its development is closely linked to the enforcement of EU policies. As early as the 1960s, the Commission recognised that the autonomy granted to Member States under the EC Treaty to sanction violations of EU law created a significant enforcement gap. Against this background, criminal law gradually assumed a functional role, primarily aimed at supporting the effective enforcement of EU policies. According to this functionalist rationale, the integration of different policy areas through EU law genuinely leads to integration in criminal law (so-called "spill-over" effect), because criminal law is necessary to address compliance deficits among Member States in implementing Community policies.

The Court of Justice of the European Union (ECJ) played a central role in facilitating and consolidating this development. Although criminal law formally belonged to national competence, the ECJ's jurisprudence imposed substantive constraints on how that competence could be exercised when enforcing Community law.[7] This dynamic gave rise to a process of indirect harmonisation of national criminal law, particularly with regard to the definition of offences and enforcement practices. Thus, Community law not only limited Member State autonomy negatively, (by precluding the application of incompatible national rules), but also positively, by requiring national systems — including prosecutorial practices and procedural rules — to meet certain standards when applied in a Community law context.

A good example of the functionalist logic underlying European criminal justice integration is the development of measures to combat cross-border crime following the abolition of internal border controls on 31 December 1992.[8] According to the functional rationale, criminal law instruments are viewed and employed as tools for addressing specific cross-border criminal threats that have emerged or intensified as a consequence of integration in other policy areas. The creation of the internal market removed physical and technical barriers to the free movement of persons, goods, services, and capital.[9] Although this development generated significant economic and social benefits, it also facilitated the expansion of cross-border criminal activities. Member States soon realised that their traditional, largely autonomous criminal justice systems were ill-equipped to address forms of criminality that extended beyond national borders in terms of commission, effects, or proceeds, e.g., drug trafficking, money laundering, human trafficking, and cybercrime. Member States therefore established mechanisms of judicial cooperation and mutual recognition of judicial decisions, while also introducing instruments to approximate substantive criminal law, including the definition of criminal offences and the setting of minimum sanctions.[10]

Historically, EU criminal law was not conceived as a deliberate constitutional project aimed at creating a comprehensive "European criminal justice system." Rather, it emerged in response to the unintended consequences of the success of the European integration process itself. Thus, the development of EU criminal law reveals a fundamental paradox: measures originally designed to facilitate the Union's primary objective of economic integration have triggered a chain of secondary effects, generating new forms of vulnerability and cross-border risks that have subsequently required further regulatory and institutional integration.[11]

Although many areas of EU integration have been identified as potentially requiring criminal law enforcement, the weakness of the functional rationale is that Member States have often been unable to reach agreement on the approximation of their national criminal laws. Indeed, several policy fields have undergone substantial approximation at the EU level without being accompanied by corresponding criminal law measures. The banking sector is a prime example. In its 2011 Communication "Towards an EU Criminal Policy", the European Commission explicitly identified banking and financial services as areas in which the role of criminal law as an enforcement tool merited further consideration.[12] The EU has made significant progress towards approximating banking regulation and creating an integrated financial framework.[13]

Yet, serious violations of banking rules have only been partially addressed through EU criminal law instruments. The rationale for criminalisation appears compelling. Given the high degree of interconnectedness of European financial markets, inadequate enforcement of EU banking rules in one Member State may have significant consequences for the stability and functioning of the financial system in others. Criminal sanctions could serve as an effective deterrent against serious misconduct, thus protecting consumers and investors, preserving confidence in financial institutions, and safeguarding the integrity and stability of the banking sector. Potential offences that could justify harmonised criminalisation at the EU level include fraudulent misuse of funds, fraudulent investment schemes, fraudulent bankruptcy, and serious violations of due diligence and compliance obligations. Nevertheless, despite the functional arguments in favour of criminal law

intervention, Member States have thus far shown limited willingness to extend EU criminal law into this field. The banking example shows that functionalist pressures do not automatically lead to approximation of criminal laws and that political considerations, concerns about national sovereignty, and divergent legal traditions continue to influence EU criminal justice integration.

Alongside the functionalist rationale, a second dimension has gradually emerged that links the development of EU criminal law more directly to the broader project of European integration itself. This constitutional dimension is often expressed in aspirational rather than purely regulatory terms.[14] It is grounded in the idea that the European Union constitutes a community of values, founded upon and committed to promoting the principles set out in Arts. 2 and 3(1) TEU. From this perspective, criminal law is not merely an instrument for addressing practical enforcement needs but also serves an important normative function. The values underlying criminal justice are complex and at times potentially conflicting.[15] The protection of legal interests through deterrence, punishment, and prevention must be pursued within a framework of fair procedures, legal certainty, and respect for individual rights. Criminal law therefore embodies both the coercive power of the state and the safeguards necessary to ensure its legitimate exercise.

In the context of the European Union, criminal law can thus be understood as a means of protecting not only specific policy objectives but also of safeguarding and actively promoting the fundamental values upon which the Union is founded. Accordingly, the development of EU criminal law should be guided by, and contribute to, the realisation of the values enshrined in Arts. 2 and 3(1) TEU. Among the values explicitly listed in Art. 2 TEU, four are particularly relevant to criminal justice: respect for human dignity, freedom, the rule of law, and respect for fundamental rights.

The emergence of this constitutional dimension was gradual. It was only with the Hague Programme that elements extending beyond a purely functional rationale began to appear in the EU's approach to criminal justice. Under its general orientations for the AFSJ, the Hague Programme acknowledged the Union's "legal obligation to ensure that in all its areas of activity, fundamental rights are not only respected but also actively promoted."[16]

A further step in this constitutional development was taken in November 2009 with the adoption of the Roadmap for Strengthening Procedural Rights of Suspected or Accused Persons in Criminal Proceedings.[17] The Roadmap, which became the foundation for the subsequent adoption of six EU Directives on procedural rights, recognised that EU action in defining minimum procedural rights was necessary to enhance mutual trust among the judicial authorities of the Member States. More importantly, however, it explicitly acknowledged that, "after a lot of progress [had] been made in the area of judicial and police cooperation on measures that facilitate prosecution," the time had come to restore the balance between enforcement objectives and the protection of individual procedural rights. This represented a significant normative development, placing the rights of suspects and accused persons at the centre of the European criminal justice project.

The constitutional dimension of EU criminal law was further elaborated in the aforementioned 2011 Commission Communication "Towards an EU Criminal Policy"[18] and in the 2012 European Parliament resolution "An EU approach to criminal law."[19] Both institutions stressed that the development of EU criminal law must be guided by the fundamental values on which the Union is founded. They highlighted the importance of safeguarding essential principles of criminal justice, including human rights protection, legality, culpability, proportionality, the presumption of innocence, *ultima ratio*, and *ne bis in idem*. Criminal law was thus increasingly presented not merely as an instrument of policy enforcement but also as a field governed by fundamental constitutional principles that reflect the Union's commitment to the rule of law and the protection of individual rights.

Adopting a values-based approach to lawmaking also offers the prospect of a more coherent and principled strategy for EU criminal law legislation. Recognising this need, the European Parliament argued in its 2012 resolution:[20]

> […] criminal law must constitute a coherent legislative system governed by a set of fundamental principles and standards of good governance in full respect of the EU Charter of Fundamental Rights, the European Convention on Human Rights and other international human rights conventions to which the Member States are signatories.

From this perspective, the constitutional dimension not only serves as a source of legitimacy for EU criminal law but also as a normative framework capable of guiding its future development in a consistent, rights-based manner.

Still, the practical implementation of this values-based approach has remained limited.[21] Although the constitutional discourse surrounding EU criminal law has become increasingly prominent, translating this normative orientation into concrete legislative and policy outcomes remains a significant challenge.[22]

III. Focus Areas for Substantive and Procedural Criminal Law

In this section, I will highlight three areas which, in my view, clearly demonstrate the need to guide the future development of EU criminal law through a value-driven rationale: (1) hate crime, (2) foreign interference with democratic processes, and (3) defence rights in the digital age. These examples are intended to be illustrative rather than exhaustive,[23] as they provide particularly compelling illustrations of the potential of a values-based approach to legislative design. Each concerns interests that are closely connected to the Union's constitutional foundations and raises questions that cannot be understood solely through the traditional logic of market integration or cross-border enforcement. Together, they demonstrate how EU criminal law can increasingly contribute to protecting the Union's core values and democratic order.

1. Hate crime and hate speech

The current EU *acquis* on hate crime remains fragmented and is characterised by a number of significant shortcomings. The central legislative instrument in this field, Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law,[24] identifies bias motivation as the defining element of hate speech and hate crime committed on racist and xenophobic grounds. However, its scope is limited. It does not extend criminal law protection to hate speech and hate crime motivated by other protected characteristics, such as sex, gender, gender identity, sexual orientation, age, disability, language, or political opinion and belief, although several Member States have chosen to include some of these grounds within their national criminal legislation. Furthermore, despite the Framework Decision being formally implemented across all EU Member States, recent analyses by the European Parliament reveal considerable disparities in national legislation, definitions, and levels of protection, resulting in an uneven landscape of hate crime regulation throughout the Union.[25]

More recently, the Directive on combating violence against women and domestic violence, adopted on 14 May 2024, has expanded EU criminal law intervention into a related area by criminalising conduct such as female genital mutilation, forced marriage, cyberharassment, cyberstalking, and certain forms of cyber incitement to hatred or violence.[26] The Directive requires Member States to criminalise the intentional incitement of violence or hatred directed against a group of persons, or a member of such a group, defined by reference to gender, where material containing such incitement is publicly disseminated by means of information and communication technologies.. The scope of the offence remains relatively narrow, however, as criminalisation may be limited to instances involving a threat to public order or conduct that is threatening, abusive, or seriously insulting.

Additional protection is provided through the Victims' Rights Directive,[27] which seeks to address the specific vulnerabilities of victims of bias-motivated offences. Pursuant to Art. 22, Member States are required to conduct an individual assessment of victims in order to determine their need for special protection measures. When performing this assessment, the competent authorities must consider the victim's personal characteristics, the nature of the offence, and the circumstances in which it was committed. The Directive expressly recognises hate crime, gender-based violence, and other offences motivated by prejudice or discrimination as categories deserving particular attention and enhanced protection for victims. While these provisions constitute an important recognition of the specific harms associated with bias-motivated offences, they primarily focus on victim protection rather than on the harmonisation of substantive criminal law.

The fight against hate speech in the online environment is further addressed through the Digital Services Act (DSA).[28] In line with the values of human dignity and respect for fundamental rights enshrined in the EU Charter of Fundamental Rights, the DSA seeks to ensure a safe, predictable, and trustworthy digital environment. The Regulation requires online platforms to establish mechanisms for the detection, reporting, and moderation of illegal content. In particular, providers of very large online platforms and very large online search engines must implement reasonable, proportionate, and effective measures to mitigate the dissemination of illegal content, including online hate speech and forms of cyber violence. The DSA does not itself define hate speech or hate crime, however, relying instead on underlying Union law and national law to determine what constitutes illegal content. As a result, divergent national definitions continue to shape the boundaries of online hate speech regulation across the Union.

From a values-based perspective, this fragmented framework appears increasingly difficult to reconcile with the Union's commitment to human dignity, equality, non-discrimination, and the protection of fundamental rights under Arts. 2 and 3 TEU. The existing *acquis* provides protection against some forms of bias-motivated offending while leaving significant gaps with regard to others. Therefore, a more coherent and comprehensive EU approach to hate crime could be justified by the need to safeguard and give

concrete effect to the Union's foundational values. Such an approach would recognise that attacks motivated by prejudice are not only offences against individual victims but also against the pluralism, equality, and mutual respect that constitute the normative foundations of the European project itself.

In this context, the Commission proposed in December 2021 that hate speech and hate crime be added to the list of particularly serious crimes with a cross-border dimension under Art. 83(1) TFEU.[29] A decision to this effect would constitute a necessary first step towards the adoption of minimum rules concerning the definition of offences and sanctions in this area, thereby enabling the development of a more coherent and comprehensive EU framework on hate crime. However, the Council has thus far failed to reach the unanimity required under Art. 83(1) TFEU to adopt the proposed decision. The lack of political consensus among the Member States has consequently stalled the formal expansion of EU criminal law competence in this area, despite growing concerns about the prevalence of hate speech and hate-motivated violence across the Union.

In response to this impasse, in December 2023, the Commission and the High Representative adopted a Joint Communication to the European Parliament and the Council entitled "No place for hate: a Europe united against hatred", setting out a broader strategy to combat hatred in Europe.[30] The Communication announced a series of initiatives spanning several policy fields, including prevention, victim support, online content moderation, awareness-raising, and improved data collection. At the same time, the Commission reiterated its call for the Council to adopt the proposed decision extending the list of EU crimes to include hate speech and hate crime, arguing that the existing legal framework remains inadequate to address evolving forms of hatred, particularly in the online environment.[31] In January 2024, the European Parliament added its support to this initiative, adopting a resolution urging the Council to include hate speech and hate crime among the areas of crime listed in Art. 83(1) TFEU, so that the Commission, in the second stage of the process, can propose minimum rules concerning the definition of criminal offences and sanctions in this area.[32]

In its Communication accompanying the proposal to add hate speech and hate crime to the areas of crime laid down in Art. 83(1) TFEU, the Commission seems to struggle to present hate speech and hate crime as serious internal security threats that are comparable to the offences currently listed in Art. 83(1) TFEU, such as terrorism, trafficking in human beings, or money laundering. Rather than focusing primarily on security concerns, the Commission emphasises the broader societal harm caused by these offences, highlighting their detrimental impact on both individuals and society as a whole and their ability to undermine the very foundations of the European Union.[33] In particular, the Communication places considerable emphasis on the threat that hate speech and hate crime pose to the Union's common values. It stresses that such conduct is fundamentally incompatible with the principles enshrined in Arts. 2 and 6 TEU and in the EU Charter of Fundamental Rights.[34] According to the Commission, hate speech and hate crime attack the values of human dignity, equality, respect for fundamental rights, and non-discrimination that constitute the normative basis of the European integration project. Therefore, the principal justification for EU action lies not only in the cross-border nature of these offences but also in their corrosive effect on the Union's constitutional order and value system.

The Commission's proposal can thus be regarded as one of the clearest and most ambitious attempts to advance the protection of EU common values through criminal law. Unlike earlier initiatives, which were predominantly justified by reference to the effective functioning of the internal market or the need to combat transnational criminality, this proposal places the safeguarding of the Union's foundational values at the centre of the argument for criminal law harmonisation. It thereby represents a significant shift towards a genuinely constitutional rationale for EU criminal law.

At the same time, however, the proposal also illustrates the political limits of a values-based approach. Under Art. 83(1) TFEU, adding new crimes to the list of "Euro-crimes" requires unanimous approval in the Council. Given the divergent views among Member States regarding the scope of hate speech regulation, freedom of expression, and the role of criminal law in protecting societal values, achieving such unanimity is likely to prove difficult.

2. Foreign information manipulation and interference

Another area that merits urgent attention from a values-based perspective is the criminalisation of foreign interference in democratic processes. Safeguarding democracy is a core objective of the European Union, intrinsically linked to the values of democracy, the rule of law, and respect for fundamental rights, as set out in Art. 2 TEU. In recent years, concerns about foreign information manipulation and interference (FIMI) have moved to the forefront of the European policy agenda. The term FIMI is now widely used to describe coordinated efforts by foreign state and non-state actors to manipulate information, distort public debate, and influence

democratic decision-making processes. The Council of Europe, the European Union, and other international organisations are currently examining the extent to which criminal law should play a role in addressing this phenomenon.[35]

While the precise scope and content of potential criminal offences require careful consideration, there can be little doubt that foreign interference has become a tangible threat to democratic governance. Numerous allegations and documented instances of information manipulation campaigns have raised concerns about their impact on national and European electoral processes. Recent experiences in several European countries, including Hungary[36] and Romania,[37] as well as concerns surrounding elections to the European Parliament, have demonstrated the vulnerability of democratic institutions to external influence and coordinated disinformation campaigns. A few European states, including Norway, Lithuania, Latvia, and Estonia, have already introduced criminal provisions specifically targeting certain forms of foreign interference, providing examples of emerging national responses to this challenge.[38]

From an EU law perspective, a key preliminary question is whether the EU has the competence to legislate in this field and, if so, what the scope of this competence is. One possible starting point would be the criminalisation of interference with EU electoral processes.[39] The rationale here would be similar to that which underpins the criminal law protection of the Union's financial interests.[40] Just as criminal law was deemed necessary to safeguard the integrity of the Union's budget, criminal law measures may be justified to protect another distinct EU legal interest: the integrity and legitimacy of European democratic processes and elections.[41]

Accordingly, Art. 83(2) TFEU could serve as a suitable legal basis for legislative action. This provision allows criminal laws to be harmonised if this is essential to ensure the effective implementation of a Union policy in an area that has already been subject to harmonisation measures. Given the importance of democratic participation and electoral integrity to the functioning of the Union, one could argue that criminal law intervention is necessary to effectively protect European elections against foreign manipulation and interference.

To some extent, aspects of FIMI that are similar to hate crime may already fall within the existing reference to "computer crime" in Art. 83(1) TFEU, particularly where online platforms, artificial intelligence, or cyber-enabled methods are used. This could also be a starting point for the criminalisation of FIMI.

3. Specific procedural safeguards adapted to the digital setting

A third example in which a values-based approach would be most pertinent for the development of EU criminal law is that of procedural safeguards. In light of the growing integration of technology, the EU should consider digitalising procedural rights where feasible, namely the rights to interpretation, translation, access to the case file, legal assistance and legal aid, and the right to be present at trial.[42] In particular, it could explore the use of videoconferencing to connect the accused with their lawyer, an interpreter, or the court itself as well as the use of artificial intelligence (AI) to ensure access to the case file or the translation of legal documents. With this in mind, the EU has funded the DigiRights (Digitalisation of Defence Rights in Criminal Proceedings) project, which aims to map and assess current digital practices surrounding these rights. The ultimate goal of the project is to propose European guidelines for the digital application of the rights.[43]

Technological developments, particularly AI, offer opportunities to not only strengthen defence rights but also to improve the accuracy of fact-finding in criminal trials. Law enforcement authorities across Europe already extensively employ AI systems both to analyse existing evidence, such as large volumes of documents, communications, and datasets[44] and to generate evidence through methods such as AI-assisted DNA analysis and facial recognition technologies.[45] These developments have the potential to enhance investigative capabilities. At the same time, however, the growing use of AI in the detection, prevention, and investigation of crime risks to create a significant imbalance of power between law enforcement authorities and the defence. The Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence illustratively describes this as "information asymmetry":[46]

> Due to certain unique characteristics of artificial intelligence systems, such as their technical complexity, their data-driven character and the relative opaqueness of the operations of some such systems, human interactions with artificial intelligence systems have been affected by the problem of opaqueness of artificial intelligence systems and information asymmetry, i.e. a significant imbalance in the access to, understanding of, or control over information between different parties involved in the activities within the lifecycle of artificial intelligence systems.

Law enforcement authorities can use AI tools to rapidly sift through large amounts of data, whereas other participants in criminal proceedings, particularly defence lawyers, often lack the infrastructure, knowledge, and means to access AI tools to carry out searches, e.g., for exculpatory evidence or for the verification of the reliability and validity of evidence.[47]

From a values-based perspective grounded in the principles of the rule of law, effective judicial protection, and the right to a fair trial, the increasing digitalisation of criminal justice therefore requires a corresponding strengthening of defence rights. To address these emerging challenges, three complementary rights should be recognised, which – together – could help preserve procedural fairness and equality of arms in an increasingly digital criminal justice environment:

- A right to digital discovery, which extends beyond the traditional right of access to the case file in order to encompasses meaningful access to relevant digital datasets and AI-generated material;
- A right to search for exculpatory evidence, which enables the defence to make effective use of digital tools and technologies in identifying evidence favourable to the accused;
- A right to digital forensic expertise, which supplements the traditional right to legal assistance by ensuring access to independent technical expertise necessary to scrutinise, verify, and challenge AI-based evidence and investigative methods.

The lack of awareness among suspects and accused persons of the use of AI during the investigation or the prosecution hinders their ability to seek an effective remedy.[48] Even though access to information about automated processing is a cornerstone principle of Regulation 679/2016[49] – particularly when a decision is "solely based on automated processing"[50] – opacity is the norm in law enforcement contexts. According to Art. 26(11) of the EU AI Act, the restrictions on the right to information set out in Art. 13 of the Law Enforcement Directive (LED)[51] also apply to high-risk AI systems used for law enforcement purposes. While Art. 13(2)(d) LED establishes an obligation to notify the data subject *ex post*,[52] it neither specifies at what stage of the proceedings this *ex post* notification should occur, nor the extent to which information must be provided.

Art. 7 Directive 2012/13/EU on the right to information in criminal proceedings[53] requires Member States to guarantee the defence access to "all material evidence in the possession of the competent authorities" and to do so "in due time to allow the effective exercise of the rights of the defence and at the latest upon submission of the merits of the accusation to the judgment of a court". However, since the Directive does not include specific guarantees tailored for digital disclosure, practices remain inconsistent across Member States. Even within individual Member States, no general rule applies: disclosure obligations vary, depending on the technology employed. To address the specificities of digital investigations, the EU should go beyond the minimum rules laid down in Art. 7 of Directive 2012/12/EU and introduce a right for the defence to access not only all the evidence but also all supplemental information necessary for their defence.[54] Some Member States have already done so in order to guarantee the equality of arms between law enforcement authorities and the defence.[55]

Finally, in order to be able to challenge the validity and reliability of AI-generated evidence, the defence needs the assistance of digital forensic experts. When paid for privately, however, this assistance can be very costly for the defendant. The existing European *acquis* on legal aid is rather limited in scope. Directive 2016/1919[56] lays down minimum common rules concerning the right to legal aid and sets a minimum standard on the quality of legal aid services. Regarding the burden of costs for legal assistance, Art. 4(1) requires Member States to ensure "that suspects and accused persons who lack sufficient resources to pay for the assistance of a lawyer have the right to legal aid when the interests of justice so require". In addition, according to Art. 7, Member States must establish an "effective legal aid system" of a "quality adequate to safeguard the fairness of the proceedings". Since lawyers are often ill-equipped to effectively assist defendants in examining digital forensic procedures, methods, and tools in AI-driven investigations, the material and temporal scope of assistance offered by the legal aid Directive must be expanded.

IV. Concluding Remarks

The evolution of EU criminal justice has always reflected the broader trajectory of European integration, with cooperation gradually and steadily intensifying due to shared values and common interests as well as the realisation that no EU Member State can effectively address contemporary criminal law challenges alone. As this contribution has demonstrated, the Union now faces a dual imperative.

On the one hand, it must address longstanding gaps in substantive and procedural criminal law, particularly in areas in which fragmentation undermines effective enforcement, such as bankingrelated offences. The recent adoption of the Regulation on European Production and Preservation Orders for electronic evidence[57] demonstrates that the functionalist rationale it is still very much present, ensuring progress and covering new ground for the future development of EU criminal law.

On the other hand, the EU must also use criminal law to promote its core values. The rule of law, fundamental rights, equality, and judicial independence are not abstract princi-

ples; they are the conditions for the legitimacy of and trust in EU criminal law without which it cannot function. Ensuring that future initiatives in this field are firmly anchored in a valuesbased approach is therefore not only normatively desirable but also practically indispensable. Mutual recognition, effective judicial cooperation, and public confidence in the Union's criminal justice project all depend on this approach.

Discussions at the HLF suggest, however, that the prospects for a stronger constitutional dimension as a guiding force in the future development of EU criminal law remain relatively limited. This is partly due to the growing divergence among Member States regarding the interpretation and practical application of shared European values. Recent years have seen serious rule-of-law concerns in several Member States, including challenges to judicial independence, political interference in the administration of justice, and broader structural deficiencies affecting the functioning of national judicial systems. In this context, the Court of Justice of the European Union has assumed an increasingly important role in safeguarding and promoting the Union's foundational values and ensuring compliance with the requirements of Art. 2 TEU. [58]

Another, and perhaps more immediate, obstacle to the development of a values-based approach is the growing fatigue among Member States regarding the implementation of new legislative measures. Since the entry into force of the Lisbon Treaty on 1 December 2009, the Union has adopted a substantial body of criminal justice legislation, covering both substantive criminal law and procedural safeguards. During the HLF discussions, a large majority of Member States indicated that the resources currently available within their ministries of justice are already fully absorbed by the task of implementing and applying the existing *acquis*. Consequently, many delegations expressed reservations about the adoption of new legislative instruments, instead emphasising the need to consolidate, streamline, and improve the coherence of the existing body of EU criminal law.

In the coming years, the challenge will therefore be to reconcile these two objectives: ensuring the effective implementation and coherence of the existing *acquis*, while also enabling EU criminal law to respond to emerging threats to the Union's constitutional values, including democracy, the rule of law, and fundamental rights. Discussions at the HLF suggest that future progress is likely to depend less on ambitious new legislative programmes and more on the strategic use of existing competencies, consistent application of the current *acquis*, and gradual development of criminal law measures capable of protecting the Union's foundational values where necessary.

Prof. Dr. Katalin Ligeti
Professor of European and International Criminal Law, University of Luxembourg

1 For the agenda of the High-Level Forum on the Future of EU Criminal Justice, see: European Commission, "High-Level Forum on the Future of EU Criminal Justice", *European Commission*, <https://commission.europa.eu/high-level-fora-justice-growth-and-future-eu-criminal-justice_en>. All hyperlinks in this article were last accessed on 10 September 2026.
2 Council of the European Union, "Presidency Conclusions, Tampere European Council, 15-16 October 1999", 16 October 1999.
3 Council of the European Union, "The Hague Programme: Strengthening Freedom, Security and Justice in the European Union", OJ C 53, 3.3.2005, 1.
4 Council of the European Union, "The Stockholm Programme – An Open and Secure Europe Serving and Protecting the Citizens", OJ C 115, 4.5.2010, 1.
5 For an overview of the post-Lisbon EU criminal law *acquis*, see Council of the European Union, *European Union Instruments in the Field of Criminal Law and Related Texts*, December 2019; Council of the European Union, "Council Conclusions on the Future of EU Criminal Law: Recommendations on the Way Forward", Doc. 10984/24, 24 June 2024, para. 1(b); P. Csonka and O. Landwehr, "10 Years after Lisbon – How 'Lisbonised' is the Substantive Criminal Law in the EU?", (2019) *eucrim* 261.
6 E. Herlin-Karnell, "All Roads Lead to Rome: The New AFSJ Package and the Trajectory to Europe 2020", (2014) *eucrim*, 28.
7 In the landmark Greek Maize case, the Court of Justice held that, although the choice of sanctions remained a matter for the Member States, national authorities were nevertheless obliged to ensure that infringements of EU law were punished under conditions analogous to those applicable to comparable breaches of national law and that the penalties imposed were effective, proportionate, and dissuasive (Case 68/88, *Commission v Greece*, ECLI:EU:C:1989:339). See further R. Sicurella, "EU Competence in Criminal Matters", in: V. Mitsilegas, M. Bergström and T. Quintel (eds.), *Research Handbook on EU Criminal Law*, 2nd ed., 2024, p. 63; K. Zoumpoulakis, "Approximation of Criminal Sanctions in the European Union: A Wild Goose Chase?", (2022) 13(3) *New Journal of European Criminal Law (NJECL)*, 341, 341-343.
8 V. Mitsilegas, *EU Criminal Law*, 2nd ed., 2022, pp. 612 ff.
9 V. Mitsilegas, *EU Criminal Law*, 2nd ed., 2022, pp. 2-4.
10 For an overview of the measures adopted by the EU, see V. Peers,

EU Justice and Home Affairs Law, Vol. II: *EU Criminal Law, Policing, and Civil Law*, 5th ed., 2023.
11 J. Monar, "Reflections on the Place of Criminal Law in the European Construction", (2021) 27(4-6) *European Law Journal,* 356.
12 Communication from the Commission, "Towards an EU Criminal Policy: Ensuring the Effective Implementation of EU Policies through Criminal Law", COM(2011) 573 final, p. 3.
13 European Commission, "What Is the Banking Union?", *European Commission*, <https://finance.ec.europa.eu/banking/banking-union/what-banking-union_en>.
14 J. Monar, (2021) 27(4-6) *European Law Journal, op. cit.* (n. 11), 356.
15 L. Mancano, "A Theory of Justice? Securing the Normative Foundations of EU Criminal Law through an Integrated Approach to Independence", (2021) 27(4-6) *European Law Journal,* 477.
16 Council of the European Union, "The Hague Programme", *op. cit.* (n. 3) p. 2.
17 Council Resolution of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, OJ C 295, 4.12.2009, 1.
18 COM(2011) 573 final, *op. cit.* (n. 12).
19 European Parliament, "Resolution of 22 May 2012 on an EU Approach to Criminal Law", OJ C 264 E, 13.9.2013.
20 European Parliament, *op. cit.* (n. 19), Recital H.
21 Indeed, beyond the adoption of the procedural rights directives aimed at strengthening defence rights in criminal proceedings, relatively few EU criminal law instruments have been primarily justified by the protection of fundamental values. While Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, OJ L, 2024/1385, 24.5.2024, represents an important development, it harmonises only a limited number of offences and, following significant political compromise during the legislative process, does not extend to key forms of gender-based violence such as rape. See M. Dell'Aquila, "Omitting Rape from the EU's Directive on Combating Violence against Women Is a Huge Mistake", *CEPS*, 28 March 2024, <https://www.ceps.eu/omitting-rape-from-the-eus-directive-on-combating-violence-against-women-is-a-huge-mistake/>.
22 See, for example, the ongoing negotiations on extending the list of EU crimes under Art. 83(1) TFEU to include hate speech and hate crime; European Parliamentary Research Service, "Hate Speech and Hate Crime: Time to Act?", PE 762.389, September 2024, pp. 9–10.
23 Other areas could equally be considered within such a framework. Indeed, at the HLF, a number of scholars, practitioners, and professional organisations advocated further EU initiatives aimed at strengthening common standards of criminal justice. Proposals included the adoption of minimum rules on detention conditions, the development of common standards governing the admissibility and exclusion of evidence, and greater approximation of investigative measures and procedural safeguards. While these initiatives differ in scope and objective, they share a common concern: the need to ensure that the AFSJ develops in a manner that reflects not only the functional demands of cooperation and mutual recognition but also the Union's commitment to the rule of law, fundamental rights, and effective judicial protection. See, e.g., See V. Costa Ramos, Guest Editorial, (2025) *eucrim* 1; S. Guerrero Palomares, "Justice Systems Built on Confidence: The CCBE Proposal on the Future of EU Criminal Justice", in this issue; T. Wahl, "Report of the High-Level Forum on the Future of EU Criminal Justice", (2025) *eucrim*, 252–254.
24 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, 55.
25 European Parliamentary Research Service, "Criminalisation of Hate Speech and Hate Crime in Selected EU Countries", PE 766.226, November 2024; European Parliamentary Research Service, "Hate Speech and Hate Crime: Time to Act?", PE 762.389, September 2024.
26 Directive (EU) 2024/1385, *op. cit.* (n. 21).
27 Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ L 315, 14.11.2012, 57.
28 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), OJ L 277, 27.10.2022, 1.
29 Annex of Communication from the Commission, "A More Inclusive and Protective Europe: Extending the List of EU Crimes to Hate Speech and Hate Crime", COM(2021) 777 final.
30 JOIN(2023) 51 final.
31 JOIN(2023) 51 final. 6.
32 European Parliament resolution of 18 January 2024, "Extending the list of EU crimes to hate speech and hate crime", P9_TA(2024)0044, OJ C, C/2024/5733, 17.10.2024.
33 The Commission invokes their impact on common values, the harm caused to individual victims and their communities, and their broader societal impact to substantiate its claim that hate speech and hate crime meet the threshold of particular seriousness required for their inclusion as an area of crime under Art. 83(1) TFEU. As regards the latter, the Commission emphasises that hate speech and hate crime "are a threat to democratic values, social stability and peace", as they "heighten social divisions, erode social cohesion, and trigger retaliation, resulting in violence and counter-violence." It further notes their "harmful impact on fundamental rights, in particular on human dignity, equality and freedom of expression." On this point, see Communication from the Commission, "A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime", COM(2021) 777 final, pp. 8–11.
34 COM(2021) 777 final, *op. cit.* (n 33), p. 8.
35 The urgency of addressing this issue is reflected in the recent Council of Europe publication, "Feasibility Study on the Possible Elaboration of a Legal Instrument on Foreign Information Manipulation and Interference (FIMI), Including Disinformation", CM/Inf(2026)18, 10 April 2026, which concludes that FIMI poses a direct threat to democracy, human rights, and the rule of law; the study recommends further work towards a Council of Europe legal instrument. See J. Kanstinger, "Committee of Ministers Gave Green Light to CoE Action on Information Manipulation and Foreign Interference", news section of this issue.
36 OSCE Office for Democratic Institutions and Human Rights (ODIHR), *Hungary, Parliamentary Elections, 12 April 2026: Interim Report*, 27 March 2026.
37 Venice Commission, *Urgent Report on the Cancellation of Election Results by Constitutional Courts*, CDL-AD(2025)003 (2025); International Foundation for Electoral Systems (IFES), *The Romanian 2024 Election Annulment: Addressing Emerging Threats to Electoral Integrity* (2024).
38 See Council of Europe, CM/Inf(2026)18, *op. cit.* (n. 35), Chapters 3, 5 and 6, discussing recent instances of foreign information manipulation and interference, their impact on democratic processes, and national legislative responses, including criminal law measures adopted in European states.
39 Significantly, the Council of Europe feasibility study (*op. cit.* (n. 35), p. 52) also identifies the protection of electoral integrity as a central objective of any future European legal instrument on FIMI.

40 This is done through 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 PIF Directive.
41 V. Mitsilegas, "The Future of EU Criminal Justice: Towards a Values-Driven European Criminal Law", (2025) 16(2) *NJECL,* 123, 124.
42 A. Klip, "The Right to Be Present Online", (2024) 32(1) *European Journal of Crime, Criminal Law and Criminal Justice* (EJCCLCJ), 1–14; S; Allegrezza and L. Bernardini, "Digitalising Judicial Cooperation in Criminal Matters: Nailed It on the First Try?", *EU Law Live*, 5 October 2024.
43 A. Beazley, *DigiRights Comparative Report*, 11 December 2025. See also European Commission, "Digitalisation of Defence Rights in Criminal Proceedings (DigiRights)", <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43252386/101056667/JUST2027>.
44 See ECJ, 30 April 2024, Case C-670/22, *M.N. (EncroChat)*, ECLI:EU:C:2024:372, concerning the large-scale cross-border collection and analysis of encrypted communications. In this regard, see also D.N. de Jonge and S.L.J. de Vries, "Data-Driven Investigations in a Cross-Border Setting", (2024) *eucrim,* 241.
45 See K. Ligeti, "Unpacking AI Evidence and (Re-)Defining Procedural Safeguards in Digital Investigations", in: K. Ligeti (ed.), *AI Evidence and Criminal Proceedings* (Oxford, Bloomsbury Publishing, 2026).
46 Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), no. 96. The report is available at: <https://rm.coe.int/1680afae67>.
47 On these questions, see K. Ligeti, *op. cit.* (n. 45).
48 For a detailed analysis of new defence rights in the context of AI evidence, see K. Ligeti, *op. cit.* (n. 45).
49 Arts. 5, 12, 13, 14, and 15 of 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). OJ L 119, 4.5.2016, 1 [hereinafter: GDPR].
50 See Art. 22 and related access rights in Arts. 15(1)(h), 14(2)(g) and 13(2)(f) GDPR.
51 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89 [hereinafter: LED].
52 Art 13(2) LED: "In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights: (a) the legal basis for the processing; (b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period; (c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations; (d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject."
53 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, 1.
54 The 'European Law Institute Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings suggests introducing a new provision into national criminal procedural law to provide that "[t]he defendant [should have] the right to access the full extent of the evidence, and to the report prepared by qualified IT experts, to challenge the chain of custody, the results of the analysis or its interpretation, and also to challenge the conclusions in the expert opinion." For the proposal, see <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>. This proposal codifies the jurisprudence of the ECtHR in *Sigurður Einarsson and Others v Iceland*, Appl. no. 39757/15 (judgement of 4 June 2019). See also the article by L. Bachmaier in this issue.
55 See, for instance, Bundesverfassungsgericht (BVerfG) [German Federal Constitutional Court], Order of 20 June 2023 – 2 BvR 1167/20, ECLI:DE:BVerfG:2023:rk20230620.2bvr116720, para. 45; District Court of Amsterdam, 27 February 2024, ECLI:NL:RBAMS:2024:686-689, 691-704.
56 Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, 1.
57 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, 118.
58 Most notably in Poland and Hungary, judicial reforms were enacted that threatened fair trial guarantees under the EU legal framework. In Case C-619/18, *Commission v Poland*, ECLI:EU:C:2019:531, the ECJ held that Poland's judicial reforms violated EU law by undermining judicial independence. In Joined Cases C-585/18, C-624/18 and C-625/18, *A.K. and Others*, ECLI:EU:C:2019:982, the Court found that Poland's Disciplinary Chamber did not satisfy the requirements of independence and impartiality under Art. 47 of the Charter of Fundamental Rights of the European Union. In Case C-286/12, *Commission v Hungary*, ECLI:EU:C:2012:687, the Court held that Hungary's legislation requiring the compulsory retirement of judges violated EU law by undermining judicial independence.

Justice Systems Built on Confidence

The CCBE Proposal on the Future of EU Criminal Justice

Salvador Guerrero Palomares

The 2025 High-Level Forum on the Future of EU Criminal Justice, aimed at developing a shared vision for the Union's future criminal-policy agenda, brought together over one hundred participants, including the Council of Bars and Law Societies of Europe (CCBE) and the European Criminal Bar Association (ECBA).
In this context, the CCBE submitted an extensive proposal, arguing that mutual recognition and judicial cooperation can only function sustainably if they are based on robust procedural safeguards that can be effectively enforced. To this end, the CCBE proposed the adoption of a new roadmap on procedural rights on the basis of Art. 82 TFEU, setting out a detailed legislative programme across four areas: *(i)* judicial cooperation and mutual recognition, *(ii)* procedural safeguards, *(iii)* EU agencies and bodies, and *(iv)* the digitalisation of criminal justice.
This article systematically presents the main strands of this proposal. In particular, it examines the reforms proposed for the European Arrest Warrant and the European Investigation Order, as well as the need for common rules on pre-trial detention and exclusionary rules for unlawfully obtained evidence. It also considers defence investigations, the strengthening of professional secrecy and legal professional privilege (attorney-client privilege), and defence safeguards in the functioning of Eurojust, Europol, and the European Public Prosecutor's Office. Lastly, it addresses the requirement for a fundamental rights-centred approach to the deployment of artificial intelligence and videoconferencing in European criminal proceedings.

I. Introduction: The High-Level Forum and the Voice of the European Legal Profession

At the beginning of 2025, the European Commission launched the High-Level Forum on the Future of EU Criminal Justice as a space for strategic reflection on the current state of European criminal justice and the regulatory priorities for a new institutional cycle after 2024. The Forum's remit focused on four interconnected areas: substantive criminal law; criminal procedure (including mutual recognition instruments); the digitalisation of criminal justice; and the role of EU agencies and bodies.

Four plenary meetings were held in 2025: on 4/5 March, 20/21 May, 1/2 October, and 1 December. These meetings brought together high-level representatives from the EU Member States, the Commission, the Council, and the European Parliament, as well as bodies and agencies such as the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO), Eurojust, Europol, the European Judicial Network (EJN), eu-LISA, and the European Union Agency for Fundamental Rights. They were joined by organisations representing civil society and justice professionals, including the European Criminal Bar Association (ECBA), the Council of Bars and Law Societies of Europe (CCBE)[1], the Confederation of European Probation, EuroPris, and the NGO Fair Trials. Leading academic experts in European criminal law and criminal procedure also participated.[2]

The CCBE, which represents the national bars and law societies of the EU Member States and other European countries at European and international levels and is regarded as the voice of the European legal profession (representing more than one million lawyers), played an active role in both the plenary sessions and in the technical debates.

In addition to oral interventions at the plenary meetings, the CCBE also contributed a written paper containing concrete proposals designed to ensure that the Union's future criminal justice policies strike the right balance between effective criminal prosecutions and the essential role of lawyers in safeguarding the rule of law and protecting fundamental rights. The paper was entitled "CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice" and was submitted on 8 October 2025.[3]

It should be emphasised that the Forum is not a decision-making body. Nevertheless, its conclusions[4] inform the Commission's considerations when drafting legislative and non-legislative recommendations. From the CCBE's perspective, the process provides a unique opportunity to place defence rights and procedural safeguards at the centre of the next phase of development of the European criminal justice system.

Against this background, the present article summarises and analyses the CCBE's proposal. Particular attention is devoted to the call for a new roadmap on procedural safeguards, targeted reforms of some of the most emblematic cooperation instruments, the role of European criminal justice agencies, and the challenges raised by the digitalisation of criminal justice.

II. The Post-Lisbon Constitutional Framework and the Need for a New Roadmap

1. The Charter of Fundamental Rights, the ECHR, and the mutual recognition principle

The CCBE's contribution is expressly grounded in the constitutional context established by the Treaty of Lisbon.

First, it relies on the Charter of Fundamental Rights of the European Union (CFR), which has the same legal value as the Treaties. Accordingly, its provisions are binding on both EU institutions and bodies – including the EPPO – and the Member States when they implement EU law. This is without prejudice to the fact that the rights guaranteed by the European Convention on Human Rights (ECHR) continue to constitute a minimum level of protection within the European legal space.

Second, the Lisbon Treaty enshrines mutual recognition of judicial decisions as the cornerstone of the Area of Freedom, Security and Justice in Arts. 67 and 82 TFEU. Mutual recognition is based on mutual trust across the Member States' judicial systems. However, this trust can only be regarded as justified where all national systems ensure comparable levels of fundamental rights protection in criminal proceedings.

Experience accumulated over more than two decades of European criminal cooperation shows that, in the absence of minimum standards, mutual recognition can lead to an almost irrebuttable presumption of uncritical acceptance of other states' decisions, even where there are serious indications of rights violations. From an institutional standpoint of the legal profession, trust cannot be imposed unconditionally; it must be built on effective guarantees.

2. From the 2009 Roadmap to a new agenda: "Justice systems built on confidence"

The 2009 Roadmap on procedural rights was a significant achievement, leading to the adoption of six key directives on interpretation and translation, information of rights, access to a lawyer, the presumption of innocence, legal aid, and specific safeguards for suspected or accused children. However, it has acknowledged that the programme remained incomplete, with new areas of vulnerability emerging in light of the technological evolution and the growing complexity of criminal cooperation.

In this context, the CCBE proposes the adoption of a new roadmap on procedural safeguards based on Art. 82 TFEU, built around the concept of "justice systems built on confidence".[5] The gradual approach of the 2009 Roadmap, which advanced through thematic instruments covering specific aspects of criminal proceedings, remains an appropriate model. The CCBE's proposal underlines that robust procedural safeguards are not an obstacle to effective prosecution, but rather a prerequisite for legally sound convictions, reduced miscarriages of justice, and strengthened public trust in criminal justice. A system that sacrifices safeguards in the name of speed will, in the medium term, generate more litigation, more appeals, and more distrust, including among the authorities of different states when they are required to recognise one another's decisions.[6]

The CCBE also cautions against the limitations of soft-law tools, such as recommendations, guidelines, best practices, and training. While such instruments can be valuable supporting measures, fundamental rights can only be effective and accessible if they are enshrined in clear, binding rules, rather than being left to administrative discretion or the goodwill of practitioners.[7]

III. Judicial Cooperation and Mutual Recognition in Criminal Matters

A central place within the agenda proposed by the CCBE is occupied by the review of the most paradigmatic mutual recognition instruments: the European Arrest Warrant and the European Investigation Order. The underlying thesis is that the effectiveness of these instruments hinges on the strength of the procedural safeguards that accompany them.

1. The European Arrest Warrant: towards a second generation

The European Arrest Warrant (EAW) is undoubtedly one of the most effective instruments of cooperation in criminal matters within Europe. Its implementation represented a qualitative leap compared with traditional extradition procedures. However, the CCBE underlines that the EAW still reflects, to a significant extent, the political and legal climate in the aftermath of the 09/11 attacks, when security concerns tended to take precedence over considerations regarding safeguards for the individual.[8]

From this perspective, the CCBE is calling for a second generation of the EAW that will fully incorporate the case law of the Court of Justice of the European Union (CJEU), the acquis developed around the Stockholm procedural-rights

roadmap, and the requirements of the Charter of Fundamental Rights. The CCBE identifies several structural shortcomings:

- Uneven protection of fundamental rights. The application of refusal grounds linked to fundamental rights varies widely among Member States. Effective protection often requires lengthy appeal proceedings, prolonging the deprivation of liberty of the requested person;[9]
- Weak proportionality control. EAWs are often issued for minor offences, for very old facts, or investigations at an early stage, leading to unnecessary arrests and the de facto use of pre-trial detention as a default measure;[10]
- Insufficient use of alternatives. Instruments such as the European Investigation Order or the European Supervision Order (ESO) are used to a very limited extent, even though they would allow the same objectives to be achieved with less impact on personal liberty;[11]
- Detention conditions and monitoring of assurances. The practice of relying on assurances regarding detention conditions communicated by the issuing State, without effectively monitoring compliance, is insufficient in light of the CJEU's case law;[12]
- Schengen Information System (SIS) alerts and compensation. The maintenance of alerts in the SIS without systematic review[13] and the absence of a harmonised compensation framework for wrongful detention in the EAW context[14] raise concerns over legal certainty.

To remedy these dysfunctions, the CCBE proposes, *inter alia,* the following*:*

- Codifying refusal grounds based on fundamental rights in line with the CJEU's case law, including a rigorous assessment of whether there is a real and individualised risk of serious rights violations[15];
- Strengthening proportionality by requiring the issuing authority to consider less intrusive alternatives before issuing an EAW and by excluding manifestly disproportionate cases;
- Promoting the effective use of the European Investigation Order and the Supervision Order as alternatives to surrender, to avoid routine recourse to deprivation of liberty;
- Establishing mechanisms for periodic review of SIS alerts and a harmonised regime of compensation for wrongful or manifestly disproportionate detention within the EAW framework.

The objective is not to weaken the EAW, but rather to anchor the instrument firmly in the protection of fundamental rights, ensuring that mutual trust is based on effective guarantees.

2. The European Investigation Order: rebalancing equality of arms

From a defence perspective, the European Investigation Order (EIO) raises certain problems that are less apparent than those of the EAW, yet equally significant. The CCBE's assessment is that there is a structural asymmetry in favour of the prosecution. This asymmetry manifests itself in several ways:[16]

- The intensity of judicial review of EIOs varies significantly between Member States; defence remedies are limited and affected persons are not always informed of the existence of an EIO;
- Access to supporting documentation is often restricted by investigation secrecy;
- Cross-border surveillance and data interception frequently expose divergences between national standards of privacy protection, which fosters *forum shopping*.[17]

Added to this are delays in the execution of EIOs, which jeopardise the right to proceedings within a reasonable timeframe and may compromise the very usefulness of the requested investigative measures.

To address these challenges, the CCBE proposes, in particular:

- Strengthening defence participation and remedies. The defence should have access to the EIO and supporting documentation, be heard on execution where appropriate, and have an effective remedy in both the issuing and executing states;[18]
- Introducing a system of dual legal representation mirroring the EAW scheme,[19] so that the person concerned is entitled to counsel in both legal orders;[20]
- Setting clearer execution timelines and legal consequences for unjustified delays, linked to the right to trial within a reasonable timeframe;[21]
- Clarifying the consequences of unlawful data interception or failure to notify affected persons through explicit exclusionary rules or equivalent safeguards;[22]
- Incorporating the principle of speciality into the EIO framework, in line with the recommendations set out in the reports of mutual evaluation on mutual recognition.[23]

IV. Strengthening Procedural Safeguards in the European Criminal Justice Area

The CCBE's contribution identifies several priority areas in which the EU should take legislative action to establish minimum standards for the protection of fundamental rights in criminal proceedings.

1. Pre-trial detention and detention conditions

Prison overcrowding and the disparity of detention conditions across Member States raise serious concerns in relation to the presumption of innocence, human dignity, and the right to a fair trial. [24]

The CCBE endorses the fundamental principle that pre-trial detention must be a measure of last resort, to be employed only where no less onerous measure can secure the legitimate aims of the proceedings.

In line with this approach, the European legal profession's contribution, pursuant to Art. 82(2) TFEU, proposes the following:

- **The establishment of a sentencing threshold** as a condition for authorising pre-trial detention, together with the requirement for **sufficient grounds**, beyond mere suspicion, of the commission of an offence and of the suspect's or accused person's responsibility; in addition, an **adequate standard** for assessing the risks that pre-trial detention is intended to prevent should be established; [25]
- **The setting of maximum time limits** on the duration of pre-trial detention, taking into account the complexity of a case, while preventing situations of prolonged deprivation of liberty in the absence of a final conviction; [26]
- **The decisive promotion of alternatives** such as conditional provisional release, electronic monitoring, or the **European Supervision Order**, which are capable of replacing pre-trial detention or reducing its length; [27]
- **The adoption of binding minimum standards on detention conditions** across the Union, insofar as they have a direct impact on the functioning of mutual recognition, particularly in relation to the **EAW**.[28]

These minimum standards should address issues such as contact with family members, access to legal and medical assistance, hygiene and nutrition, and cell size. More generally, they should also cover all aspects relating to respect for human dignity in places of detention.

The CCBE also proposes the innovative measure of recognising **inspection powers** for deans of bar associations and their delegates, enabling the verification of detention conditions first-hand to engage in a structured dialogue with penitentiary authorities. [29] It also advocates establishing a **European preventive mechanism**, inspired by national mechanisms as set out in the 2002 Optional Protocol to the UN Convention against Torture. Unlike the usual practice of the European Committee for the Prevention of Torture, this mechanism would have the power to conduct **unannounced inspections.**[30]

The message is clear: improving detention conditions and reducing recourse to pre-trial detention are not only fundamental rights imperatives, but also an indispensable prerequisite for the credibility of mutual recognition in criminal matters—a point not remedied by the non-binding Recommendation 2023/681[31].[32]

2. Exclusionary rules: closing a critical gap

According to the CCBE, one of the most striking deficits of the Union's current criminal procedural acquis is the absence of common minimum rules on the exclusion of unlawfully obtained evidence, despite Art. 82(2)(a) TFEU expressly envisaging the adoption of rules on the mutual admissibility of evidence.

In a European criminal justice area where evidence circulates relatively easily between Member States, the lack of shared criteria governing the consequences of rights violations when evidence is gathered generates profound legal uncertainty. This has become particularly evident in recent cases involving the mass collection of electronic communications data, such as the well-known "EncroChat" and "Sky ECC" cases.[33]

In this context, the CCBE identified several problems:[34]

- There is no general obligation under EU law to exclude evidence obtained through serious violations of fundamental rights;
- National legal systems adopt markedly divergent approaches, ranging from near-automatic exclusion of evidence to broad admissibility subject to subsequent balancing of interests;
- In practice, the principle of "non-interference" is frequently applied, meaning that evidence obtained in accordance with the law of the place of collection is admitted in the criminal proceedings of the forum even if this would breach the safeguards established by the latter;
- The procedural remedies available to the defence to challenge the lawfulness of cross-border evidence are fragmented and largely ineffective.

Based on these findings, the CCBE endorses a proposal developed by the European Law Institute, which combines two elements:[35] (1) the application of the *lex loci regit actum* principle, whereby evidence is deemed lawful if obtained in accordance with the law of the place of collection, subject to verification by the authorities and the defence in the forum; and (2) a safeguard clause permitting exclusion where the use of the evidence in the forum would conflict with its fundamental constitutional principles.[36]

Additionally, and in accordance with the ECtHR's case law, the CCBE's contribution asserts that certain categories of evidence should be considered absolutely inadmissible in all circumstances. This includes evidence obtained by torture or ill-treatment; evidence gathered in violation of the privilege against self-incrimination; and evidence secured through deception that gravely undermines the person's free will.

Regarding other interferences with rights, the CCBE calls for the adoption of common proportionality criteria, inspired by the CJEU's doctrine and certain national experiences. These criteria include:[37]

- A clear legal basis for the measure;
- Prior judicial authorisation or, if this is not possible, immediate judicial ratification;
- Specificity of the measure as regards the person under investigation and the relevant facts;
- Exceptionality of the measure meaning that less intrusive measures are unavailable;
- Necessity and proportionality *stricto sensu*.

The purpose of this framework is not to fully harmonise national evidentiary rules, but rather to establish a minimum core of protection against the circulation of evidence obtained under weaker safeguards, thereby preventing criminal cooperation from becoming a means of "importing" lower standards.

3. Professional secrecy and legal professional privilege / attorney–client privilege

Professional secrecy and legal professional privilege/attorney–client privilege occupy a central place in the CCBE's proposal. While there is a general agreement on their importance in the abstract, national regimes differ significantly in terms of their substantive scope, legal force, and practical application,[38] particularly in contexts involving the fight against organised crime or terrorism.

The contribution recalls that the CJEU has long recognised the confidentiality of communications between lawyers and clients as a general principle of EU law,[39] and that the case law of both the CJEU and the ECtHR – interpreting Arts. 7 and 47 of the Charter and Art. 8 ECHR – underscores its structural role in the right to a fair trial.[40]

However, the absence of any specific EU-level regulation leaves Member States a wide margin of discretion. Recent events in certain countries — including the *Kulák v Slovakia* case before the ECtHR[41] – demonstrate that, without a common framework, the protection of professional secrecy can be undermined by search, seizure or interception practices that treat lawyers as sources of information about their clients.[42]

The CCBE therefore proposes the adoption of minimum standards under Art. 82 TFEU that address, *inter alia,* the following:[43]

- Searches of law offices, with reinforced safeguards regarding judicial authorisation, the presence of representatives of the Bar, and document-filtering (screening) mechanisms;
- An explicit rule rendering inadmissible evidence obtained in breach of professional secrecy, with clear exclusionary effects;
- Specific guarantees for situations in which lawyers are involved as witnesses or even as suspects, to prevent the lawyer's position from being used to undermine the privilege attaching to other clients.

These orientations are structured around six principles elaborated by *Holger Matt* and taken up in the CCBE's proposal: [44]

- Strong legal protection of professional secrecy;
- Absolute confidentiality in criminal defence matters;
- Strict limits on client waivers of privilege;
- Reinforced procedural safeguards (sealing of documents, intervention by the Bar, and screening mechanisms);
- A client's right to remain silent regarding privileged communications;
- Extension of protection to lawyers' collaborators and staff.

4. The presence of counsel during searches and seizures

The effectiveness of defence rights should not be confined to the trial hearing; it must also extend to critical stages of the investigation, such as searches and seizures of homes, offices, or electronic devices.

While Directive 2013/48/EU recognises the right of access to a lawyer during certain investigative measures, many national legal systems interpret its catalogue restrictively and do not acknowledge a clear right for counsel to be present during searches.[45]

The CCBE contends that this practice accords neither with the letter nor with the spirit of the Directive, nor with the CJEU's and the ECtHR's case law.[46] Searches expose the person concerned to risks of self-incrimination and are often conducted in contexts of intense emotional pressure. In

such circumstances, information about rights, including the right to remain silent under Directive 2012/13/EU, may be purely formal in the absence of effective legal advice.

In this regard, the contribution proposes amending Directive 2013/48/EU so as to explicitly include searches and seizures in the list of measures during which the suspect or accused has (at minimum) a right to the presence of counsel. Practical objections, namely the need to commence a search without delay, can be addressed through a balanced design combining the following points:[47]

- An obligation to notify known counsel of the imminent search;
- The right of the person concerned to request the appointment of a lawyer if none has yet been instructed;
- The possibility of commencing the search immediately, even before counsel arrives, provided that the opportunity for subsequent review is preserved and that the measure is properly documented.

This ensures a reasonable balance between investigative needs and the protection of defence rights at a particularly sensitive stage.

5. Defence investigations

The CCBE's contribution devotes specific attention to defence investigations, the possibility and legal validity of which are regarded as an essential component of the principle of equality of arms.[48] In many legal systems, the existing normative and practical framework is strongly oriented towards prosecution-led investigation, whereas the defence lacks a clear framework for gathering evidence on its own initiative.[49]

In the absence of regulation, evidence obtained by the defence may be deemed inadmissible or "unlawful", which discourages its collection and weakens the adversarial nature of proceedings.[50] In this regard, the CCBE refers to the ECtHR judgment in *Vasaráb and Paulus v Slovakia*, in which the conviction was based exclusively on prosecution evidence and none of the defence's numerous evidentiary requests were admitted.[51]

Against this background, the CCBE argues that properly regulated defence investigations could entail the following:[52]

- Enhance the effectiveness and fairness of proceedings by enabling the confrontation of alternative accounts of the facts;
- Reduce the workload of public authorities by enabling certain measures to be initiated directly by the defence and then reviewed under judicial oversight;
- Facilitate early resolution of cases by providing the defence with objective information with which to advise clients realistically about procedural risks.

Accordingly, the proposal calls for a European framework that recognises the right of defence counsel to conduct investigations in both domestic and cross-border proceedings and that establishes clear criteria for the admissibility of evidence thus obtained. The ultimate aim is to incorporate the adversarial process model more coherently into the European criminal justice system for the benefit of equality of arms.

6. Freezing and confiscation of assets

The CCBE's contribution also examines the framework established by Directive 2014/42/EU governing the freezing and confiscation of instrumentalities and proceeds of crime in the EU.[53] The main criticism concerns is that, while the Directive requires the immediate return of frozen assets which are ultimately not confiscated, it leaves to national legislation the determination of the specific conditions for restitution, the maximum duration of freezing measures, and the rules on compensation for harm caused.[54]

This lack of harmonisation raises significant concerns regarding legal certainty and equal treatment. Notably, it could lead to substantial interference with the right to property, for instance if bank accounts, business assets or property necessary for the exercise of a profession are frozen for prolonged periods without a commensurate compensation regime.

The CCBE proposes that the Union address these shortcomings through the following measures:[55]

- Setting maximum time limits for freezing measures, calibrated to the procedural stage and the complexity of the case, yet always designed to avoid the unjustified prolongation of interference;
- Establishing minimum compensation standards, including an automatic baseline indemnity calculated as an annual percentage of the value of the frozen asset, where the freezing measure ends without confiscation, with the possibility of higher compensation where the owner substantiates greater loss.

This scheme aims to strike an appropriate balance between the need for effective tools to recover criminal assets and protecting property rights and ensuring legal certainty for those affected, particularly in cross-border contexts where delays inherent in mutual recognition may extend the duration of freezing measures.

7. Conflicts of jurisdiction and legal certainty

In the CCBE's words, the determination of the competent jurisdiction is the "starting point" for the protection of human rights and procedural safeguards, given that the level of protection can vary significantly between Member States.[56] Nevertheless, the current framework for conflicts of jurisdiction, structured around Framework Decision 2009/948/JHA[57], relies on voluntary consultations between authorities and lacks binding resolution mechanisms.

In the CCBE's view, this system facilitates the following:[58]
- Forum shopping, whereby authorities select the jurisdiction most favourable to their interests;
- Situations of legal uncertainty for persons under investigation who may face parallel proceedings;
- Potential infringements of the *ne bis in idem* principle;
- Practical inefficiencies where no authority is willing to assume responsibility for the case.

It is notable that the Union has adopted a detailed Regulation on jurisdictional conflicts in civil and commercial matters (Regulation 1215/2012);[59] yet in criminal matters, the issue is left to a soft-cooperation instrument, supplemented by non-binding Eurojust guidance.

Against this background, the CCBE proposes the adoption of a Regulation on conflicts of jurisdiction in criminal matters, establishing the following:[60]
- Clear criteria for the allocation of jurisdiction, inspired by principles, such as proximity, the unity of proceedings, and the protection of the affected person;
- An obligation to adopt a formal judicial decision on jurisdiction, challengeable both by the person under investigation and, where applicable, by the victim;
- Mechanisms designed to prevent forum shopping and to ensure respect for the *ne bis in idem* principle throughout the Area of Freedom, Security and Justice.

Such an instrument would make a decisive contribution to strengthening legal certainty – a core element of the rule of law – and, consequently, mutual trust between national systems.

V. EU Agencies and Bodies: Transparency, Oversight, and Defence Rights

The third part of the CCBE's contribution focuses on the role of Eurojust, Europol, and the European Public Prosecutor's Office (EPPO) within the Union's criminal justice architecture.

While their important contribution to combating serious cross-border crime is acknowledged, a number of reservations are expressed regarding transparency and defence safeguards in relation to their activities.[61]

The principal challenges identified are:[62]
- The existence of interventions that significantly affect the situation of suspects or accused persons, such as coordination decisions, recommendations on jurisdiction, or the identification of investigative targets, which are not adequately documented or accessible to the parties;
- The lack of clarity and of specific safeguards governing data exchanges between Eurojust, the EPPO, Europol, and national authorities;
- The fragmentation of oversight mechanisms and the presence of grey areas of responsibility in complex operations involving multiple actors.

Far from advocating unrestricted access to sensitive operational information, the CCBE argues that interventions by these agencies that have a material impact on individuals' rights should be subject to standards of documentation, reasoning, and review compatible with Art. 47 of the Charter (the right to an effective remedy).

In particular, the CCBE's contribution recommends that any initiative aimed at strengthening the role of Eurojust or the EPPO should be accompanied by:[63]
- Explicit recognition of defence rights and equality of arms within their legal frameworks;
- An obligation to formally record interventions affecting a person's procedural position, so that the chain of decisions can be reconstructed;
- The creation of access mechanisms enabling lawyers to request clarification or to challenge the agency's action(s) before a competent authority, thereby preventing potential rights violations;
- The consolidation of safeguards in data exchanges to ensure that any transfer and use of information complies with the principles of legality, purpose limitation, proportionality, and legal certainty;
- The establishment or reinforcement of independent oversight bodies with specific fundamental rights competences, which are particularly relevant in contexts involving the large-scale processing of digital data;
- The possibility of resorting to a "special advocate" or "special counsel", who is independent of the main defence but subject to judicial control, to examine sensitive information whose direct disclosure to the parties might compromise ongoing investigations;
- The establishment of a complaints mechanism that al-

lows affected individuals to challenge unjustified or disproportionate interventions by Eurojust or the EPPO.

These proposals reflect a basic logic: the greater the operational weight of European criminal agencies in prosecutorial practice, the greater the density of defence safeguards, transparency mechanisms, and avenues of accountability must be.[64]

VI. Digitalisation of Criminal Justice: Artificial Intelligence and Videoconferencing

The fourth and final part of the CCBE contribution addresses the challenges posed by the digitalisation of criminal justice. It pays particular attention to the use of artificial intelligence (AI) tools and the increasing acceptance of videoconferencing in criminal proceedings, including cross-border ones.

1. Artificial intelligence in criminal proceedings

The CCBE acknowledges the potential of AI and other digital tools to enhance the efficiency of criminal justice, for example, by screening large volumes of data, conducting forensic analysis of electronic devices, and identifying behavioural patterns. It cautions, however, that deploying them in criminal law contexts entails significant risks for fundamental rights, equality of arms, and the integrity of proceedings.

As regards digital and AI-derived evidence, the CCBE calls for the adoption of EU rules that ensure:[65]

- Clear reliability and transparency criteria for the tools employed, including sufficient information on their methodologies and margins of error;
- Rigorous preservation of the data chain of custody, from collection through to presentation at trial;
- The defence's right to access, review, and challenge evidence generated or processed by AI systems, including access to relevant technical documentation to the extent necessary for the effective exercise of adversarial proceedings.

The CCBE further stresses that judicial decision-making must remain in human hands.[66] AI may perform support functions, such as organising information, flagging patterns, and suggesting hypotheses, but it must not replace human judgment or erode the judge's personal responsibility. Under no circumstances should AI tools be used in ways that undermine the presumption of innocence, the right to privacy, data protection, or the confidentiality of lawyer–client communications. The CCBE rejects the use of predictive techniques in criminal investigations.[67]

In line with these principles, the CCBE advocates for the establishment of a specific regulatory framework for the use of AI in criminal justice that is grounded in human rights, transparency, and accountability. It also calls for the prohibition of high-risk technologies, such as certain forms of predictive AI and profiling in criminal matters, as these technologies may generate structural biases and opaque decisions that are difficult to subject to effective scrutiny.[68]

2. Videoconferencing in cross-border criminal proceedings

Videoconferencing has become a widely used tool in criminal proceedings, both domestic and cross-border, particularly in the wake of the COVID-19 pandemic. Its advantages in terms of saving time and costs are evident. The CCBE cautions, however, against a trend towards normalising its use, as this could undermine fundamental safeguards.[69]

The positions set out in the contribution can be summarised as follows:[70]

- Videoconferencing should be the exception in hearings on the merits. It should not be used for budgetary reasons alone, nor where there are well-founded doubts as to its compatibility with a fair trial;
- Its use should be conditional upon informed consent by the accused, with access to legal advice, and the right to challenge decisions to hold a remote hearing;
- Harmonised safeguards must be established to protect the confidentiality of lawyer–client communications during videoconference hearings. The unlawful interception of such communications should be criminalised;
- The physical presence of counsel alongside the accused plays a crucial role in preventing pressure or intimidation, especially where the accused is in custody. The ability to examine witnesses face-to-face should not be sacrificed where it is necessary to the fairness of the proceedings;
- It is essential to establish minimum technical standards at Union level to ensure the most faithful reproduction possible of in-person interaction, including: adequate audio and video quality to capture nuances of testimony and body language; secure transmission and document management systems; and the presence of an independent person, such as a court officer, alongside the remote participant to verify identity and certify the conduct of the hearing.
- The deployment of videoconferencing requires appropriate training programmes for judges, prosecutors, law-

yers, and other practitioners. These programmes should focus not only on the technical operation of the tools but also on identifying the risks that their use may pose to fundamental rights.

The guiding principle is clear: technology must serve justice, not the reverse. The digitalisation of criminal justice will only be legitimate if embedded in a normative framework that preserves, and ideally strengthens, the procedural safeguards of the criminal process.

VII. Conclusions: From Soft Law to Binding Safeguards

The CCBE's contribution to the High-Level Forum on the Future of EU Criminal Justice provides a coherent and structured vision of a criminal justice system within the Union, in which mutual recognition is genuinely built on trust. However, this trust cannot be presumed; it must be underpinned by robust, enforceable, and effective procedural safeguards.

At the core of this vision is the proposal for a new roadmap on procedural safeguards under Art. 82 TFEU. Rather than relying exclusively on soft-law instruments and on the mere execution of existing measures, the CCBE is calling for progress towards binding minimum standards in areas such as pre-trial detention and detention conditions, exclusionary rules for unlawfully obtained evidence, professional secrecy and legal professional privilege/attorney–client privilege, defence investigations, and the presence of counsel during searches and seizures.

In parallel, the proposal emphasises that significant adjustments are required to the flagship instruments of mutual recognition — the European Arrest Warrant, the European Investigation Order and the framework governing conflicts of jurisdiction— in order to fully accommodate the requirements of the Charter and the case law of the European courts. A more fundamental rights-compliant European Arrest Warrant, a European Investigation Order that ensures equality of arms, and a regulation on conflicts of jurisdiction would consolidate mutual trust.

At the institutional level, strengthening the role of Eurojust, Europol, and the European Public Prosecutor's Office must necessarily be accompanied by reinforced guarantees of transparency, defence rights, and accountability. Criminal cooperation cannot be based on *a priori* presumptions of respect for fundamental rights and institutionally embedded procedural safeguards; rather, it must be based on clear and reviewable procedures.

Finally, the digitalisation of criminal justice — particularly through the use of artificial intelligence and videoconferencing — requires a proportionate regulatory response that combines openness to innovation with a firm commitment to fundamental rights. The European Union therefore finds itself at a crossroads: It can either pursue the purely instrumental modernisation of criminal justice centred on efficiency, or it can seize the opportunity to reaffirm the rule of law and the centrality of procedural safeguards at the very heart of the integration project.

The CCBE's proposal clearly aligns with the latter approach. Viewed from the perspective of the legal profession and scholarship on criminal procedure, the CCBE's contribution, drawn up by its Criminal Law Committee, offers a realistic, yet ambitious blueprint for a future EU criminal procedural law worth its name: a body of law that balances effectiveness and justice, enables the effective prosecution of serious crimes without compromising human dignity, and transforms mutual trust into more than a rhetorical formula.

1 In its French acronym: Le Conseil des Barreaux Européens.
2 Including Professors Valsamis Mitsilegas (University of Liverpool), Katalin Ligeti (University of Luxembourg), Lorena Bachmaier Winter (Complutense University of Madrid), and André Klip (Maastricht University).
3 Cf: Council of Bars and Law Societes of Europe, *CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice*, 8 October 2025, available at: <https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/CRIMINAL_LAW/CRM_Position_papers/EN_CRM_20251008_CCBE-contribution-to-the-High-Level-Forum-on-the-Future-of-EU-Criminal-Justice.pdf> accessed 18 May 2026.
4 Cf. T. Wahl, "Report of the High-Level Forum on the Future of EU Criminal Justice", <https://eucrim.eu/news/report-of-the-high-level-forum-on-the-future-of-eu-criminal-justice/>, accessed 18 May 2026.
5 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), p. 3.
6 Ibid., p. 3.
7 Ibid., p. 3.
8 Ibid., p. 7.
9 Ibid., pp. 8–9.
10 Ibid., p. 10.
11 Ibid., p. 13.
12 Ibid., p. 13.
13 Ibid., p. 13.
14 Ibid., pp. 11–12, expressly following S. Guerrero Palomares, "La reforma de los instrumentos de reconocimiento mutuo a la luz de la

Dr Salvador Guerrero Palomares
Chair of the CCBE Criminal Law Committee; Partner at GUERRERO ABOGADOS; Associate Lecturer in Procedural Law at the University of Malaga (UMA); Member of the CCBE Permanent Delegation to the European Court of Human Rights

jurisprudencia del TJUE", in: A. Hernández López and E. Laro González (eds.), *Proceso Penal Europeo: ultimas tendencias, analisis y perspectivas*, 2024, pp. 304–306.
15 See well-known judgments such as 5 April 2016, Aranyosi and Caldararu, C-404/15 and C-659/15, and the more recent judgment of 31 January 2023, Puig Gordi and Others, C-158/21.
16 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, 8 October 2025, pp. 14–17.
17 This expression seeks to reflect the ability of investigative authorities in cross-border cases to choose the most favourable jurisdiction – in this context, the one offering weaker protection of the rights and safeguards of the suspect or accused.
18 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), pp. 15–16.
19 Art. 10 of Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings, OJ L 294, 6.11.2013, 1.
20 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), p. 17.
21 Ibid., p. 15.
22 Ibid., pp. 17–18.
23 Ibid., p. 18. Reference is made to the Council Final Report of 10 December 2024 on the tenth round of mutual evaluations on the application of the European Investigation Order (EIO).
24 Ibid., p. 22.
25 Ibid., pp. 24–25.
26 Ibid., p. 25.
27 Ibid., p. 25.
28 Ibid., pp. 25–26.
29 Ibid., p. 26.
30 Ibid., pp. 27–28.
31 Commission Recommendation (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detention and on material detention conditions, OJ L 86, 24.3.2023, 44.
32 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), pp. 23–24.
33 Ibid., p. 27. For the cases, see also M. Lassalle and S. Lannier, "EncroChat – A Judicial Chronology", 4/2025 eucrim; T. Wahl, "What Remains of the ordre public in Transnational Surveillance?", 4/2025 eucrim.
34 Ibid., p. 28.
35 Ibid., p. 29.
36 An explanation of the European Law Institute proposal can be found in: L. Bachmaier Winter, "The Quest for Evidentiary Rules in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights", in: L. Bachmaier Winter and F. Salimi (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings*, 2024, pp. 1 ff. See also L. Bachmaier, "Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings", (2023) *eucrim*, 223–229.
37 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), pp. 29–30.
38 L. Bachmaier Winter and S. C. Thaman, "A Comparative View of the Right to Counsel and the Protection of Attorney-Client Privilege Communications", in: L. Bachmaier Winter, S.C. Thaman, and V. Lynn (eds.), *The Right to Counsel and the Protection of Attorney-Client Privilege in Criminal Proceedings: A Comparative View*, 2020, p. 7, pp. 37–69.
39 Cf.: ECJ, 18 May 1982, *AM&S v Commission*.
40 ECtHR, 25 March 1992, *Campbell v. the United Kingdom*, Appl. no. 13590/88; ECtHR, 6 December 2012, *Michaud v France*, Appl. no. 12323/11; ECtHR, 3 February 2015, *Apostu v Rumania*, Appl. no. 22765/12.
41 ECtHR, 3 April 2025, *Kulák v Slovakia*, Appl. no. 57748/21.
42 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), p. 31.
43 Ibid., p. 32.
44 Ibid., pp. 32–33. These principles was exposed by Prof. Holger Matt in a seminar held in Marbella (Málaga), October 2024 in an ERA seminar.
45 Ibid., p. 34.
46 Ibid., pp. 34–35.
47 Ibid., p. 35.
48 Ibid., p. 36.
49 The CCBE contribution relies on the report by E. Sellier and A. Weyembergh, *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, 2018, commissioned by the European Parliament (LIBE Committee), available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604977/IPOL_STU(2018)604977_EN.pdf> accessed 18 May 2026.
50 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), p. 38.
51 Ibid., p. 38.
52 Ibid., p. 38.
53 OJ L 127, 29.4.2014, 39.
54 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), p. 39.
55 Ibid., pp. 39–40.
56 Ibid., p. 40.
57 Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, OJ L 328, 15.12.2009, 42.
58 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), p. 40.
59 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351, 20.12.2012, 1.
60 CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, *op. cit.* (n. 3), pp. 40–41.
61 Ibid., p. 42.
62 Ibid., p. 42.
63 Ibid., pp. 43–44.
64 Ibid., p. 44.
65 Ibid., p. 48.
66 Ibid., p. 49.
67 Ibid., p. 49.
68 Ibid., pp. 49–50.
69 Ibid., p. 50.
70 Ibid., pp. 51–52.

Towards a New Roadmap for Defence Rights

The ECBA's Vision for the Future of EU Criminal Justice

Vânia Costa Ramos, Amedeo Barletta and Elise Martin-Vignerte

Over more than two decades, the EU's area of criminal justice has been built instrument by instrument — a forest of interdependent legal tools. Yet the ecosystem is out of balance: enforcement powers and prosecutorial instruments have grown vigorously while the procedural safeguards designed to protect individuals remain underdeveloped, poorly harmonised, and increasingly strained by digital evidence, cross-border investigations, and the widening operational role of EU justice and home affairs agencies. This system must be improved, and the European Criminal Bar Association (ECBA) outlined its vision in its Agenda for European Criminal Justice, prepared for the 2025 High-Level Forum on the Future of EU Criminal Justice (HLF). This article summarises that intervention. Drawing on the Agenda, it presents both a short-term programme to improve existing instruments and a long-term vision envisaging for a coherent, rights-based European criminal justice framework grounded in genuine equality of arms. It pays particular attention to three intersecting themes that crystallised in the ECBA's discussions with practitioners: the Lisbonisation and coherence of the mutual recognition framework; the role of the European Public Prosecutor's Office (EPPO) and the need for harmonised procedural safeguards in cross-border proceedings; and the potential of video-conferencing and non-custodial measures to reduce the structural overuse of pre-trial detention. The article concludes with concrete legislative demands.

I. Introduction: The Forest and Its Fault Lines

In October 2025, the European Criminal Bar Association (ECBA) presented its Agenda for European Criminal Justice entitled "Redefining EU Criminal Justice: a Vision for a Fairer System".[1] Prepared in anticipation of the third meeting of the High-Level Forum on the Future of EU Criminal Justice (HLF), the document offered a significant institutional opportunity to advance these priorities at the highest political level.[2]

The Agenda describes the EU's criminal law framework as a living ecosystem: "a forest of legislation designed to protect its inhabitants from criminal behaviour and ensure their defence rights." While this metaphor is apt, it also highlights a structural issue. A forest in which some trees are generously watered while others wither produces imbalance rather than vitality. The ECBA's core contention, developed through years of engagement with practitioners, is that the EU's criminal justice forest has been cultivated with systemic asymmetry: mutual recognition instruments and prosecutorial tools have flourished, while the procedural safeguards and defence rights that lend legitimacy to the system have been left in the shade.

The consequence is fragmentation. Many issues are governed by each EU Member State's law, leading to different procedures and procedural outcomes. These include whether a suspect whose assets haven been frozen can access the case file; whether a lawyer can attend a search of their client's home; whether the suspect or accused receives a copy of a seized digital device; whether intercepted communications are admissible in subsequent prosecutions; whether evidence may be obtained through hacking; whether a person of limited means may choose their own lawyer in a cross-border case; and whether a defendant living in another Member State can attend the trial remotely.

The 2009 Stockholm Roadmap produced six Directives on procedural rights.[3] They brought long-needed structure, but the framework remains under construction and progress has stalled. Meanwhile, the EU criminal justice landscape has evolved dramatically: the European Public Prosecutor's Office (EPPO) is operational, mutual recognition instruments have multiplied, digital evidence has come to dominate investigations, and the mandates of Europol and Eurojust have expanded. The Lisbon Treaty transformed judicial cooperation from a fragmented, intergovernmental system into a constitutionalised area of EU law, strengthening democratic oversight, enhancing the role of the Court of Justice of the European Union (CJEU), and anchoring fundamental rights at the core of cooperation. However, the system still resembles a patchwork: framework decisions, directives, and regulations having been developed incrementally and often lacking coherence and interoperability, creating legal uncertainty and uneven protection of rights across Member States.

The HLF, launched in February 2025, was an institutional response to this context. Among defence practitioners and civil society organisations, the ECBA, the CCBE, and Fair Trials were formally invited and took part throughout the Fo-

rum's work. The ECBA engaged actively: it attended every plenary meeting and, in November 2025, submitted detailed written comments on the draft final report, building directly on its Agenda for European Criminal Justice.

This article presents the ECBA's intervention at the HLF.[4] As outlined in the Agenda, the ECBA's approach is structured around two tracks: the first ("the protective embrace of the forest's trees") addresses existing instruments that require targeted repair; the second ("a healthy forest to ensure our future") concerns the coherent, long-term architecture that the EU must build. Three intersecting themes run through both tracks and are reviewed in this article:

- The need for the Lisbonisation and coherence of the mutual recognition framework;
- The structural gaps exposed by the EPPO's operation;
- The transformative potential of video-conferencing technology and non-custodial supervision measures to reduce the overuse of detention, in particular in cross-border settings.

II. Track One (Immediate Interventions): Repairing the Existing Instruments

1. Lisbonisation and coherence: From patchwork to an integrated system

The Lisbon Treaty profoundly changed the constitutional framework of EU criminal justice, yet instruments in place before Lisbon, most notably the Framework Decision on the European Arrest Warrant (FD EAW) have not been systematically updated to reflect that transformation. This has resulted in a structural mismatch: instruments designed under the intergovernmental logic of the third pillar (under the Amsterdam/Nice framework) now operate within a constitutionalised legal order that imposes compliance with the EU Charter of Fundamental Rights (CFR), full CJEU jurisdiction, and democratic oversight by the European Parliament. Recasting these instruments is therefore not merely a technical exercise but a constitutional and structural imperative.

The ECBA's Agenda therefore calls for either a comprehensive instrument consolidating the *acquis* or, at minimum, clearer rules on how instruments relate to one another and on their subsidiary application. No measure adopted under one instrument should undermine rights guaranteed under another. Each new legislative act in EU criminal law should include a mandatory cross-reference provision to applicable safeguards to ensure its application does not lead to decisions that violate other EU legal instruments. Explicit rules on interaction and conflict resolution, alongside a requirement for integrated, proportionate application (making detention the last resort rather than the default) would have positive systemic effects beyond the formal legal framework, including less pre-trial detention and prison overcrowding, and a more proportionate use of coercive measures overall.

At the HLF, the ECBA presented this as the overarching principle underpinning its entire intervention: "any extension or strengthening of enforcement measures must be accompanied by reinforcement of procedural safeguards and defence rights to preserve equality of arms and fairness of the procedure".[5] Mutual trust, the foundation of the EU's judicial cooperation architecture, cannot be sustained by instruments that operate in silos. Rather, it requires a coherent framework in which rights and obligations are clearly articulated, instruments interact predictably, and individuals can rely on consistent protections regardless of which instrument is invoked or in which Member State proceeding are brought.

2. The European Arrest Warrant: A tree that requires a trim

The ECBA describes the European Arrest Warrant (EAW) as "one of the oldest trees in the forest" that "requires a trim to flourish." From a Member State's perspective, the EAW system is a success story. From the defence perspective, however, this is less certain. The gradual recognition of a fundamental rights exception by CJEU case-law, since *Aranyosi* and *Căldăraru*,[6] has not resolved the instrument's structural deficiencies. The EAW has become the default tool even when less intrusive alternatives would suffice; it is frequently used for investigative purposes, for minor offences, or on stale facts, resulting in serious personal and financial costs for the accused and for the public purse.

During the HLF, the ECBA urged the European Commission and the Member States to undertake a long-overdue revision of the FD EAW, aligning it with CJEU case law and curbing disproportionate use. The proposed reform should encompass the following:

- A case-specific proportionality test at the issuing stage, based on the likely custodial sentence to be delivered rather than the statutory maximum;
- A consultation procedure, modelled on the Directive relating to the European Investigation Order (EIO), allowing the executing state to trigger less coercive alternatives, such as an EIO or a European Supervision Order (ESO);
- The codification of human rights violations as an explicit, mandatory ground for refusal to surrender;
- A fully-fledged right to dual defence[7] and legal aid;

- A mandatory video-link hearing after arrest, enabling the issuing state to either maintain the EAW or to request an alternative measure;
- Guaranteed access to the case file in the issuing state without delay;
- Rules for cross-border summons and hearings by video-link to reduce reliance on the EAW at the investigative stage;
- A right of appeal against surrender decisions;
- Mutual recognition of decisions refusing surrender;
- An independent, EU-level mechanism to regulate the issuance and continued validity of Schengen Information System (SIS) alerts.

The vast majority of Member States at the Forum took the position that no legislative revision of the EAW is necessary, arguing that reliance on the CJEU's evolving case-law has been a sufficient corrective. The ECBA rejected this approach on both principled and practical grounds: First, CJEU's case-law is no substitute for clear, binding legislative standards that issuing authorities and requested persons can rely on with certainty. Second, the European Parliament called for legislative action as far back as 2014; a decade later, that call remains unanswered.

3. Mutual recognition of refusal decisions: A seedling to nurture

The Agenda identifies the absence of mutual recognition of refusal decisions as a "seedling" in urgent need of nurturing. When one Member State has refused to surrender a person (e.g., on grounds of *ne bis in idem*, fundamental rights, or proportionality), this decision has no binding effect on other Member States. A person whose extradition has been refused in Member State A on EU-wide grounds can nevertheless be arrested, detained, and surrendered upon entering Member State B, facing renewed deprivation of liberty in each jurisdiction and effectively turning free movement under Art. 21 TFEU into a source of legal jeopardy.

The ECBA's proposals address this gap directly.[8] A refusal based on *ne bis in idem*, on grounds pursuant to Recital 12 of the FD EAW, or on the proportionality principle should have permanent, EU-wide effect, binding all Member States. A refusal based on the risk of ill-treatment contrary to Art. 19 CFR or of a flagrant denial of justice should likewise be binding on all Member States until evidence that the risk no longer exists is provided. Once a permanent refusal decision has been issued, the creation or continued processing of data in the SIS or through Interpol's Red Notices system should be prohibited, with effective judicial remedies available for breaches.

4. The EIO and the coherence of the mutual recognition framework

Beyond the EAW, the ECBA advocated a systematic approach to the EU's entire mutual recognition framework. The current patchwork of instruments creates conditions for forum shopping, generates legal uncertainty, and incentivises the circumvention of safeguards through instrument choice. The EAW and the EIO should not be treated as interchangeable; their relationship should be governed by an explicit subsidiarity principle requiring prior consideration and, where appropriate, use of the less coercive instrument. For the EIO specifically, the ECBA reiterated the need to reinforce defence rights in cross-border investigations through dual legal representation and a robust principle of speciality.

The ECBA also raised the need to improve the legal framework governing Joint Investigation Teams (JITs), as the absence of clear rules on applicable law and access to JIT documentation creates room to circumvent both national and EU safeguards. Proper regulation of the cross-border service of procedural documents would reduce the disproportionate reliance on the EAW and prevent trials in absentia, which violate Directive 2016/343.

III. Track Two (the Long-Term Vision): Cultivating a Coherent Forest

1. Procedural safeguards: Where the forest is thinnest

Of all the pillars of the HLF, procedural safeguards generated the greatest divergence of positions between Member States, on the one hand, and defence lawyers' associations, academics, and civil society, on the other. The key issues discussed were:

- **Pre-trial detention.** The ECBA stresses that there is a clear EU legal basis for action on detention, in particular pre-trial detention (Art. 82(2)(b) TFEU) and urges the adoption of binding EU standards of protection. Data from the European Committee for the Prevention of Torture and Inhuman and Degrading Treatment of Punishment (CPT) confirm that no Member State fully complies in practice with European detention standards. Various sources have documented prison overcrowding and the disproportionate use of pre-trial detention as a default rather than a last resort.[9] At the HLF, representatives from the Member States unanimously opposed binding action at EU level. The Forum's conclusions, which call for further soft-law measures, amount to a deferral rather than a response, given that a non-binding Recommenda-

tion has been in place since 2022 without resolving the underlying structural problem.

- **Legal professional privilege.** EU law provides no harmonised standard for the protection of legal professional privilege in criminal proceedings. In a cross-border environment marked by pervasive digital surveillance and EU agency involvement, this gap creates serious risks for lawyer-client communications. The ECBA therefore advocates binding EU rules to protect legal professional privilege, with particular attention to digital evidence, where the protection of privileged information is crucial.
- **Admissibility of evidence and exclusionary rules.** Although Member States accepted recommendations from the High-Level Group on Access to Data to develop EU minimum rules on mutual admissibility of prosecution evidence derived from interception of communications, those same Member States firmly opposed EU legislative action on exclusionary rules and defence-side admissibility standards. In the ECBA's view, it is unacceptable to seek expanded, harmonised capacities to retain and use communications data while refusing to legislate on the admissibility of such data as evidence, or on the exclusion of unlawfully obtained material thereby jeopardising fair trial rights.

2. The EPPO: Cross-border evidence, defence rights, and the limits of harmonisation

The establishment of the EPPO marks a paradigm shift: for the first time, the EU exercises direct prosecutorial powers across borders. However, this development exposes structural gaps. The EU still lacks a fully harmonised framework for gathering evidence across borders. Divergences in national procedures raise serious questions about the admissibility and lawfulness of evidence, as well as equality of arms. These issues are particularly pertinent in EPPO proceedings, as they by definition span multiple jurisdictions, each with its own rules on investigative measures, judicial authorisation and evidentiary standards.

In this context, defence rights must be strengthened, not diluted. The ECBA emphasises the need for consistent procedural safeguards, effective remedies (including exclusionary rules for unlawfully obtained evidence), and access to legal aid across borders. Without these measures, EPPO proceedings risk exacerbating existing inequalities. The final HLF report noted that defence lawyers' associations emphasised the need for stronger procedural safeguards in EPPO cases.[10]

The urgency is compounded by proposals to extend the EPPO's competence to violations of EU restrictive measures, which would add further complexity to its multi-jurisdictional workload. Therefore, any revision of the EPPO Regulation should establish explicit and binding procedural rights for the suspect and accused, including access to the file in the pre-trial phase, judicial review of EPPO investigative decisions, and harmonised standards for particularly intrusive investigative measures – especially the gathering of e-evidence and the use of AI-processed material.

3. Video-conferencing: A proportionality tool, not a convenience

Video-conferencing has evolved from a pandemic-era workaround to an increasingly normalised feature of cross-border criminal proceedings. The ECBA's position is clear:[11] video-links can be valuable tools, but virtual presence is not equivalent to physical presence and, if used without proper safeguards, risk undermining fair trial rights.

From a proportionality perspective, the potential of video-conferencing in a cross-border setting is significant. For example, a mandatory video-conferencing hearing after arrest under an EAW would allow the issuing state to reassess whether surrender remains necessary and proportionate. Could the suspect or accused be interviewed? Could alternative measures be ordered? Should the EAW be maintained or replaced by supervision or an EIO? This single procedural step could substantially reduce the use of EAWs for investigative purposes, which currently account for a substantial share of those issued. Similarly, clear EU rules allowing suspects or accused persons residing in another Member State to be heard via video-link at pre-trial, investigative, and certain trial hearings – without prejudice to the right to be present in person – would reduce pressure to arrest and detain individuals solely to secure attendance.

Video-link also offers solutions to mitigate the risks posed by trials in absentia. It can facilitate participation from another Member State, potentially avoiding surrender while preserving meaningful procedural involvement – provided that the accused retains the right to consent or refuse participation, interpretation is available where needed, and technical standards ensure reliable identification and secure, confidential lawyer–client communication.

That said, video-conferencing cannot substitute for the right to be physically present at trial. Participation in a trial by video-link should always require the accused's informed and express consent. Parity of arms in technology. ensuring comparable tools, quality, and connectivity for prosecution and defence, must also be guaranteed.

4. Non-custodial measures: Rethinking supervision to reduce detention

A structural reform of the EU's non-custodial supervision instruments is one of the most discussed priorities. The European Supervision Order (ESO) was designed to allow suspects and accused persons to remain in their Member State of residence under supervision as an alternative to pre-trial detention. Despite its advantages, including enhancing proportionality, reducing unnecessary deprivation of liberty, and enabling individuals to prepare their defence more effectively, the ESO remains seriously underused in practice.

The reasons for this are well documented: the lack of a mandatory proportionality assessment in respect of the non-use of the measure, complex procedures, a lack of awareness among practitioners, weak operational cooperation between issuing and executing authorities, and the absence of direct supervision mechanisms.[12] The ECBA therefore calls for a fundamental rethink of how these instruments operate. Rather than relying solely on the executing state to organise supervision – a process that is slow, resource-intensive, and often unfamiliar to local authorities – consider schemes in which the issuing state retains direct supervisory responsibility while the person remains in their Member State of residence, with assistance from local law enforcement and probation authorities as needed. Such arrangements should be placed on an EU legal footing to ensure consistency, accountability, and genuine operational uptake.

Another underused mechanism is house arrest with electronic monitoring as an alternative to pre-trial detention. Several Member States already employ it domestically as a standard alternative to pre-trial detention.[13] At EU level, no harmonised framework governs such measures in cross-border cases. The ECBA considers it timely to explore the legal feasibility and operational benefits of establishing minimum EU standards for house arrest with electronic monitoring as an alternative to pre-trial detention in cross-border settings. This would help alleviate prison overcrowding and reduce the personal and financial costs of unnecessary detention, while maintaining the person's connection to their home, family, and legal counsel.

These proposals should not be treated as secondary. Overcrowding and the overuse of pre-trial detention are one of the most serious systemic failings of European criminal justice.[14] Addressing it requires both binding minimum standards and operational instruments that make non-custodial alternatives genuinely viable. A reformed ESO, a direct supervision framework, and harmonised electronic-monitoring standards are the practical instruments through which the principle of detention as ultima ratio can be given real effect.

5. Digitalisation: Efficiency in service of fairness

On digitalisation, the ECBA's proposals strike a balance between embracing the potential of digital tools and insisting on clear safeguards for their deployment. The Agenda emphasises that digitalisation should not be an end in itself but a means to fairer and more effective proceedings, in full compliance with procedural safeguards and defence rights.

On artificial intelligence (AI), the ECBA warns against dehumanising criminal justice through over-reliance on technology and identifies specific high-risk applications, such as predictive policing (risk of algorithmic bias), sentencing and parole tools (opacity/"black box" issues), and digital forensics relying on large datasets without defence access to the underlying data. The ECBA recommends that any framework for the responsible use of AI include the following:

- Clear ethical guidelines based on international standards;
- Transparency, documentation, and independent third-party audits;
- Meaningful human oversight and accountability;
- Disclosure of AI involvement in decisions;
- Limits on AI for core judicial acts;
- Safeguards for the presumption of innocence and non-discrimination.

Beyond this, during the HLF, a digital mechanism to check whether parallel related cases are pending was discussed. was discussed. The ECBA proposed expanding it in order to enable the defence to ascertain whether multiple proceedings for the same facts are underway and to verify whether closed proceedings in another Member State support a *ne bis in idem* argument.

6. EU JHA Agencies: Expanding power, lagging accountability

While the operational powers of the EU's justice and home affairs agencies Europol, Eurojust, and the EPPO have expanded, the framework for judicial oversight and accountability has not kept pace. At the Forum, the ECBA reiterated the governing principle of its Agenda's (see II.2 above): there should be no further expansion of these agencies' powers without commensurate safeguards. The ECBA called for a stronger framework for judicial control at EU level and for structured communication channels with Eurojust and the EPPO, which would enable defence lawyers to request infor-

mation, challenge jurisdictional decisions, and participate meaningfully in processes affecting their clients.

7. Substantive criminal law: Values-based, not security-centred

On the future of substantive criminal law is concerned, the ECBA adopted a position of principled selectivity. While endorsing the Forum's evidence-based approach and welcoming a more values-based orientation over a purely security-centred one, it opposed broad expansion of EU-level approximation of substantive criminal law. Such expansion often makes national criminal law frameworks more rigid, sometimes hindering appropriate decriminalisation, affecting the principle of subsidiarity, and impeding the necessary narrowing of offence definitions. The ECBA's contribution focused on three themes: robust *ne bis in idem* protections, the need for coordinated EU reflection on AI-enabled crime, and the insistence that legislative speed must not come at the expense of legality, foreseeability, and proportionality .

IV. The Forum's Balance Sheet: Progress Made, Work Remaining

The HLF's final report is, as it openly acknowledges, a synthesis of "sometimes contradictory views".[15] It documents Member States' systematic preference for soft law on defence rights, in contrast to their readiness to accept binding standards when law enforcement is the beneficiary. The ECBA regrets the lack of openness by Member States at the HLF and the very limited outcomes in this area, notably the exclusion of matters relating to pre-trial detention. The ECBA will continue to advocate for binding rules and urges the EU legislature to establish a permanent forum that includes defence stakeholders and continues to address the issues discussed at the HLF.

V. Conclusion: Five Legislative Demands for the Next Institutional Cycle

The ECBA's Agenda for European Criminal Justice concludes with a call that is both diagnosis and programme: a new EU roadmap that would provide a vision for the future and keep the forest healthy. This requires closing gaps, ensuring coherence and interoperability of the judicial cooperation instruments (EAW, EIO, ESO), adapting to emerging trends, and promoting strong procedural safeguards. Without a clear plan, confidence in the EU criminal justice system – and the Union more broadly – will erode, jeopardising mutual trust on which cooperation depends.

The ECBA therefore calls on the European Commission and the European Union legislature to pursue the following five concrete legislative priorities in the current institutional cycle:

- **Lisbonisation and coherence of the mutual recognition framework.** Pre-Lisbon framework decisions should be recast into a coherent, post-Lisbon system with explicit rules on how instruments interact, a mandatory subsidiarity principle requiring the least coercive measure available to be considered first, and a proportionality requirement making detention genuinely a measure of last resort. The systemic effects would be substantial, including reduced pre-trial detention, less prison overcrowding, and a more proportionate use of coercive measures overall.
- **Amendment of the EPPO Regulation** to enshrine explicit procedural rights for the suspect and accused and to harmonise evidence-gathering standards. This should include binding rules on access to the case file in the pre-trial phase; mandatory prior judicial authorisation for intrusive investigative measures; clear standards for the collection and admissibility of e-evidence; clear standards for the use of AI-processed material and the outputs of surveillance measures; and effective judicial review of EPPO investigative decisions by competent national courts.
- **A dedicated EU instrument on the use of video-conferencing in criminal proceedings.** This instrument should establish:
  - The right of the accused to request a video-link hearing in cross-border proceedings and require a mandatory video-link hearing after arrest under an EAW to allow the issuing state to decide whether to maintain the warrant or seek alternatives;
  - Rules for remote participation in investigative hearings and, subject to the suspect or accused's consent; lay down technical and procedural standards, including confidentiality of lawyer–client communication and reliable identification to ensure fairness;
  - A proportionality requirement to ensure that video-links serve as a tool to reduce unnecessary detention and other coercive measures.
- **Reform of the European Supervision Order and European Probation Framework** to increase operational uptake and make non-custodial alternatives genuinely viable. This should include:
  - An EU legal basis for direct supervision schemes, under which the issuing state retains supervisory responsibility for the individual in their state of residence, with possible assistance from local enforcement and probation authorities;
  - An assessment of the legal feasibility of harmonising

house arrest with electronic monitoring as a standard alternative to pre-trial detention in cross-border settings; these rules should build on the experience of Member States that already use electronic-monitoring schemes in domestic proceedings.

- **Harmonised minimum standards for pre-trial detention** that include the use of house arrest with electronic monitoring as an alternative. Based on Art. 82(2)(b) TFEU and justified by evidence from the EU Fundamental Rights Agency, the CJEU case-law on detention conditions, and persistent overcrowding of pre-trial detention facilities across the EU, these standards should set clear rules on conditions, duration, and judicial review of pre-trial detention, and require a mandatory proportionality assessment to determine whether the same objectives could be achieved with less harm by using house arrest with electronic monitoring.

Justice in Europe must be about more than just efficiency. Justice in Europe must protect individuals not only from crime but also from arbitrary interference, disproportionate intrusion, and inequality before the law. Reaffirming the centrality of the rule of law and fundamental rights within the EU criminal justice system – in short, placing them at the very heart of the forest – is essential to achieving a genuine Area of Freedom, Security and Justice. This needs to be the standard against which the EU legislature's post-HLF actions are ultimately judged.

Vânia Costa Ramos
Chair of the European Criminal Bar Association (ECBA), Defence lawyer (Portugal)

Amedeo Barletta
Vice-Chair of the European Criminal Bar Association (ECBA), Defence lawyer (Italy)

photo: © Guido Athmer

Elise Martin-Vignerte
Board Member of the European Criminal Bar Association (ECBA), Solicitor and Policy Advisor for the Law Society of Ireland

photo: © Guido Athmer

* The authors would like to thank all ECBA members who contributed to the discussions on the future of European criminal justice.

1 The Agenda is available at: <https://www.ecba.org/extdocserv/projects/ECBA%E2%80%99sAgendaforEuropeanJustice.pdf>. All hyperlinks in this article were last accessed on 4 August 2026.

2 See also the ECBA's press release on the Agenda at: <https://www.ecba.org/content/index.php/publications/statements-and-press-releases/951-the-ecba-s-agenda-for-european-criminal-justice-redefining-eu-criminal-justice-a-vision-for-a-fairer-system-october-2025>.

3 The Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings outlined key areas where action should be taken at EU level to strengthen procedural defence rights. This Roadmap led to the adoption of 6 directives on the rights to interpretation and translation, to information, to access to a lawyer, to legal aid, the protection of the presumption of innocence, and procedural safeguards for children suspected or accused in criminal proceedings.

4 The ECBA's interventions at the HLF were based on: the ECBA's Agenda for European Criminal Justice, *op. cit.* (n. 1); the ECBA's written comments on the draft Report of the High-Level Forum on the Future of EU Criminal Justice, submitted to the European Commission on 5 November 2025; the Report of the High-Level Forum on the Future of EU Criminal Justice of 1 December 2025; the Guest Editorial published by Vânia Costa Ramos in eucrim 1/2025, 1; and internal ECBA practitioner discussions. The oral interventions of the Chair and ECBA Vice-Chair at the four HLF plenary sessions are also reflected throughout this article.

5 Verbal intervention by Vania Costa Ramos at the high-level forum.

6 CJEU, 5 April 2016, Joined Cases C-404/15 and C-659/15 PPU, *Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen*.

7 One could even argue for a broader concept of "total or global defence", including not only the issuing state and executing state but any relevant jurisdiction – see, for the context of EPPO proceedings, V. Costa Ramos, "The EPPO and the equality of arms between the prosecutor and the defence". (2023) 14(1) *New Journal of European Criminal Law (NJECL)*, 43, 55–57.

8 See ECBA Statement on Mutual Recognition of Extradition Decisions at : <https://ecba.org/extdocserv/publ/ECBA_STATEMENT_Mutualrecognitionextraditiondecisions_21June2022.pdf>.

9 For example, see European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT), *35th Annual Report on its activities (2025)*, p. 11, available at: <https://rm.coe.int/48802b585f>; K. Kamber, "The overuse of pre-trial detention as a public policy and human rights problem", *Confederation of European Probation (CEP)*, <https://www.cep-probation.org/the-overuse-of-pre-trial-detention-as-a-public-policy-and-human-rights-problem/>; Prison Insider, "Concrete to counter overcrowding? The figures and realities behind the rhetoric", 15 July 2025, <https://www.prison-insider.com/en/articles/le-beton-contre-la-surpopulation>; I. Aydinoglu, "Beyond capacity: Europe's prison overcrowding challenge", *Penal Reform International*, 11 December 2024, <https://www.penalreform.org/blog/beyond-ca-

pacity-europes-prison-overcrowding-challenge/>. See also, UN, *United Nations System Common Position on Incarceration*, April 2021, <https://www.un.org/ruleoflaw/wp-content/uploads/2021/12/UN_System_Common_Position_on_Incarceration.pdf>.

10 See Report of the High-Level Forum on the Future of EU Criminal Justice, <https://commission.europa.eu/document/download/606f0f38-12f9-4893-8941-3ac835229bcd_en?filename=-JUST_template_comingsoon_standard_16.pdf>, pp. 16–17.

11 This approach was developed in the Agenda, *op. cit.* (n. 1) as well as in the ECBA's Statement of Principles on the use of Video-Conferencing in Criminal Cases in a Post-Covid-19 World, 6 September 2020, available at: <https://www.ecba.org/extdocserv/20200906_ECBAStatement_videolink.pdf>, and in its survey of criminal defence lawyers on the use of video-conferencing in criminal and European Arrest Warrant proceedings, 2024, available at: <https://www.ecba.org/extdocserv/projects/Cyber/202410_9_ECBA%20_Feedback_criminal-defenselawyers_variousEUstates.pdf>.

12 See for example, V. Glerum and H. Kijlstra, "Overarching Analysis", *Mutual Recognition 2.0 Research Project*, <https://mutualrecognition-nextlevel.eu/sites/mutualrecognition/files/2025-06/MR%202.0%20Overarching%20Analysis.pdf>; pp. 89–92, 101, 139. M. Daliani, Factsheet on the European Supervision Order, *EPHESUS*, <https://www.ephesus-project.eu/uploads/1/4/4/7/144711219/1._eso_factsheet_en_v01.pdf>; Fair Trials, "Blog: Why are alternatives to the European Arrest Warrant not being used?", 8 April 2021, <https://www.fairtrials.org/articles/news/blog-why-are-alternatives-european-arrest-warrant-not-being-used/>; E. Sellier and A. Weyembergh (eds.), *Criminal procedures and cross-border cooperation in the EU area of criminal justice, Comparative study*, 2020, <https://library.oapen.org/bitstream/handle/20.500.12657/40047/9782800417219.pdf?sequence=1&isAllowed=y>, pp. 341–345; A.M. Neira-Pena, "The Reasons Behind the Failure of the European Supervision Order: The Defeat of Liberty versus Security", (2020) 5(3) *European Papers*, 1493–1509, available at: <https://www.europeanpapers.eu/system/files/pdf_version/EP_EF_2020_I_042_Ana_Maria_Neira_Pena_00402.pdf>.

13 J. Burchett and A. Weyembergh, *Prisons and detention conditions in the EU*, February 2023, <https://www.europarl.europa.eu/RegData/etudes/STUD/2023/741374/IPOL_STU(2023)741374_EN.pdf>, p. 83; see also, W. Hammerschick, "D2.2 Pre-trial detention alternatives: Best practices", *PRE-TRIAD Project – Alternative pre-trial detention measures*, 2021, <https://www.uibk.ac.at/media/filer_public/8f/0c/8f0c02ec-44c7-46ab-be88-839b07db8a3b/d22-pre-trial-detention-alternatives-best-practices.pdf>, pp. 33–36, who alerts though to the risks of net-widening when not used as a true alternative to pre-trial detention.

14 Council of Europe, "Serious overcrowding and increasing proportions of older and women detainees in European prisons – Council of Europe's 2025 penal statistics for the continent published", <https://www.coe.int/en/web/portal/-/serious-overcrowding-and-increasing-proportions-of-older-and-women-detainees-in-european-prisons>; CPT, 35th Annual Report on its activities (2025), *op. cit.* (n. 9).

15 See High Level Forum Report, *op. cit.* (n. 10), p. 6.

Rethinking Procedural Safeguards in the Digital Age

Bulk Surveillance, Artificial Intelligence, and the Need for Responses at the EU Level

Lorena Bachmaier Winter

This article examines the impact of digitalisation, mass surveillance, and artificial intelligence (AI) on procedural safeguards in criminal proceedings in the context of the developments in the EU's Area of Freedoms, Security and Justice. The author argues that contemporary surveillance capacities are changing the way in which prevention, intelligence, and criminal investigation are related to one another. Prior to the commencement of formal proceedings, individuals may be classified as "persons of interest" or "pre-suspects" via bulk data processing, algorithmic risk assessments, and communications interception, usually without the safeguards attached to suspect status. The article begins with an overview of ECtHR case law regarding secret and bulk surveillance, as well as the interception of communications for security purposes. Next, the focus is put on the CJEU ruling in *EncroChat* and its implications for transnational electronic evidence, access to communications of non-suspects, and the defence's ability to challenge the lawfulness, authenticity, and integrity of data obtained from encrypted platforms.

The author draws attention to the fact that the analysis of bulk data, coupled with AI capacities, may weaken the requirement of prior suspicion and undermine adversarial guarantees when data gathered outside of criminal proceedings is later used as incriminating evidence. She concludes that European legal systems must rethink procedural safeguards for the digital age, strengthening controls over reasonable suspicion and regulating algorithmic suspicion and mass data analysis. They must also address the role of private technology companies in criminal investigations. This would best be achieved at the EU level, as the bloc continues to develop its Area of Freedom, Security and Justice, always seeking to strike the right balance between fighting crime efficiently and ensuring procedural safeguards.

I. Introduction

The digitalisation of every aspect of our lives is a driving force for change in contemporary society, impacting all areas. This article examines the extent to which digitalisation is being properly "steered" by our legal systems. This is done from the perspective of procedural safeguards in criminal proceedings, which must revolve around human dignity and the protection of fundamental rights. The issue is becoming increasingly relevant – and urgent – in light of the populist and autocratic tendencies in many legal orders previously considered to be firmly committed to the principles of the rule of law.

The following sections will analyse some of the problems and tensions that contemporary criminal proceedings face in the digital era. This analysis will help us rethink the future of criminal procedure in a "digitalised" world and explore how we can continue to safeguard individuals against the State's increasingly all-embracing power. I will not address the – albeit highly relevant – topics of the use of technology in general and the rules on electronic evidence or videoconferencing. The aim of this article is rather to draw attention to the ways in which information and communication technologies – particularly the State's capacity for mass surveillance, which is set in motion long before criminal proceedings formally commence – are already transforming the structure and functions of criminal proceedings.[1]

Two factors require us to reconsider the safeguards of the criminal justice system. The first factor concerns "persons of interest" who are subject to certain surveillance measures that may affect their right to privacy and their right to data protection. As they are not suspects in a criminal investigation and no criminal proceedings have been formally initiated, however, the corresponding safeguards do not apply. Still, it is evident that their situation is not comparable to that of an ordinary citizen who is outside the attention of security systems. Finding the appropriate balance between protecting individuals from the State and allowing the identification of risks that may significantly impact their liberty and privacy is difficult.[2] In parallel, data acquired through surveillance measures may be used in the criminal proceedings to trigger suspicion and investigative measures or even as evidence.

The second factor is the enormous expansion of surveillance possibilities through digital technologies and sophisticated software using artificial intelligence and, in the near future, quantum computing. These developments are changing the scope of preventive and predictive surveillance, as the information gathering of the "pre-digital age" – through informants, police surveillance, or the interception of communications by intelligence services – becomes less relevant.[3]

In this context, the role of large tech companies cannot be overlooked — not only because of their capacity to interfere with our right to privacy, but also because, they are becoming necessary "partners" of law enforcement authorities in criminal investigations through their management of our data.[4]

Without aspiring to find answers to all emerging questions of this digital revolution, in the following sections, I will highlight the need to redefine procedural safeguards in a digitalised context, namely where the fields of prevention and prosecution have become increasingly blurred. As it stands, AI tools are enabling the processing of vast amounts of data, which could affect both the initiation and the outcome of a criminal proceeding. To set the scene, I will first outline the current approaches of the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU) regarding mass surveillance and access to bulk data without prior suspicion of an individual (Section II). Second, I will identify the main challenges for the criminal proceedings in the digital environment(Section III). Finally, I will draw conclusions for the future of procedural safeguards in the European Union (Section IV).

II. Intelligence, Prevention, and the Bulk Interception of Communications — From *Big Brother Watch* to *EncroChat*

The scenario described in the introduction raises several questions concerning the definition of suspects' rights in national codes of criminal procedure, also considering that only a minimum level of harmonisation at the EU level has been achieved through the procedural rights directives. Should we consider defining and regulating rights of individuals who are classified as persons of interest or "pre-suspects"? Do the safeguards provided by the data protection and data retention rules adequately protect citizens' rights? Should a new level of safeguards be introduced for these individuals to ensure that data collected for security purposes is not used for criminal prosecution? Should additional safeguards beyond those foreseen in criminal proceedings be required for the processing of data obtained through bulk surveillance?

The case law of the ECtHR (1. below) provides some guidance to these questions, even though the ECtHR has gener-

ally left the neuralgic issue of the admissibility of evidence in cases of procedural rights violations up to the national laws. The CJEU has also established some building blocks (2. below) and, in contrast to the ECtHR, even introduced some relevant criteria on the admissibility of digital evidence.

1. The case law of the ECtHR

The ECtHR established in numerous judgments the minimum standards of rights that must be guaranteed to individuals in the context of the protection of national security. Since *Klass and Others v. Germany*,[5] the ECtHR's approach has focused on the safeguards that must accompany methods of secret surveillance (covert surveillance), as well as how each of those investigative activities is recorded. The requirements relating to the interception of communications involving mass surveillance were defined in *Szabó and Vissy v. Hungary*,[6] *Weber and Saravia v. Germany*,[7] and *Zakharov v. Russia*,[8] but the Court has rarely assessed whether a situation affects national security. It has, however, stated that the protection of national security must always be weighed against the seriousness of the intrusion into the individual right to respect for private life.

a) The *Big Brother Watch* case

The opportunity to analyse mass surveillance measures and the right to privacy was given in the *10 Human Rights Organizations v. United Kingdom* case,[9] better known as the *Big Brother Watch* case. The applicants specifically argued that Art. 8 of the UK Regulation of Investigatory Powers Act (RIPA) 2000, which allowed the surveillance of bulk interceptions (through programmes such as KARMA POLICE, Black Hole, TEMPORA, etc.), did not comply with the standards set out in the ECtHR's previous case law.[10]

In its analysis of the *Big Brother Watch* case, the Court reiterated: [11]

> [T]he lawfulness of the interference is closely related to the question whether the 'necessity' test has been complied with and it is therefore appropriate for the Court to address jointly the 'in accordance with the law' and 'necessity' requirements.

However, the Court did not merely invoke its earlier case law on bulk interceptions, but also assessed whether that case law from ten years earlier was still applicable to the present digital environment.[12] The Court concluded that a new approach was required, as not all the safeguards for interceptions directed against specific persons are applicable in the case of bulk interceptions, for example the requirement of probable cause.[13]

Before analysing the specific safeguards that must be adopted for the bulk interception of communications, the Court outlined the different stages of this measure: (1) the initial search for information, which takes place for the most part in an automated manner; (2) the application of selectors; (3) the analyst's initial examination of the material resulting from the search, following the application of the selectors; and (4) the use of the intercepted material. It then specified that control mechanisms and effective safeguards must be present at each stage.

According to the Court, "the process must be subject to 'end-to-end safeguards', meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken."[14] The Court paid particular attention to the aforementioned second stage, the "application of selectors," as this stage is especially sensitive, since the choice of selectors may trigger the interception against individual persons.[15] It confirmed that states can use measures for the bulk interception of communications and that each member state must delimit the scope of application, depending on their needs assessment in terms of national security.

In contrast to the Grand Chamber majority, not all of the judges were convinced by the argument that information obtained through bulk interception would have no evidential impact. As expressed in the joint, partly concurring opinion:[16]

> It appears that on the basis of the information thus obtained, law enforcement agencies could act, for example, by proceeding to conduct investigative measures or even arrests, this in turn producing evidence for the purpose of prosecution. It is likely that in a not so distant future, by exploring this particular ground, crime investigation might move from targeted surveillance to bulk interception of data.

This statement can only be endorsed, as evidenced by the rapid development of AI tools since this judgment was issued.

b) Subsequent case law

The ECtHR has subsequently ruled in several cases on the extent to which systems for the interception of communications, whether preventive in nature or operated by intelligence services, comply with the ECHR, specifically the right to respect for private life recognised in Art. 8 ECHR. In the judgment in *Ekimdzhiev and Others v. Bulgaria*,[17] the Court held that there had been a violation of Art. 8 ECHR due to the lack of adequate legal provisions ensuring that secret surveillance — and the subsequent system for the retention of and access to the intercepted communications — was limited to what was strictly necessary.

In *Haščák v. Slovakia*,[18] the Court found a violation of Art. 8 ECHR due to the lack of safeguards against arbitrary interferences, as required by the principles of the rule of law, and the fact that the retention of the intercepted communications had not been subject to external supervision.

Similarly, in *Pietrzak and Bychawska-Siniarska v. Poland,*[19] involving surveillance measures adopted preventively under Poland's anti-terrorism legislation, the ECtHR confirmed a violation of Art. 8 ECHR, due to the lack of adequate supervision of communications monitoring carried out under anti-terrorism legislation.

c) The *ByLock* case

Another important case is the *Yüksel Yalçinkaya v. Turkey* case,[20] also known as the *ByLock* case or the "Turkish *EncroChat"*. The case concerned the use of evidence that was obtained from access to an encrypted communication system, questioning the admissibility of evidence and its conformity with Arts. 6 and 8 ECHR. The applicant alleged that the lack of judicial control over the obtaining and processing of data from the *ByLock* platform made it impossible to verify the authenticity and integrity of those electronic communications. Despite this evidence having been decisive and incriminating, the defence was unable to challenge its reliability, authenticity, and lawfulness.

The ECtHR first reiterated its general doctrine on the admissibility of evidence, i.e., that the assessment of evidence is essentially a matter for the national courts and that the Court's role is limited to reviewing whether that assessment is unreasonable or arbitrary, since the ECtHR is not a fourth instance. The reasoning of the national judgment should shed light on these matters. Regarding the use of the encrypted communication system, in this case, the ECtHR stated that the mere downloading or using such a system, or even the use of any other method to safeguard the private nature of the messages exchanged, neither constitutes a criminal offence in itself (in this case membership of a terrorist organisation), nor can it be considered an evidential element capable of convincing an objective observer that unlawful activity or even a criminal offence is being committed.[21]

Having analysed the manner in which the evidence had been obtained, the safeguards adopted in respect of the integrity and authenticity of the evidence, and the response to the accused's appeals, the ECtHR concluded that Art. 6(1) ECHR had been violated. The Strasbourg Court did not call into question the legitimacy of access to the *ByLock* platform. On the contrary, it stated: [22]

> The use of electronic evidence showing that an individual is using an encrypted messaging system that has been specifically designed and used exclusively by a criminal organisation in the internal communications of a criminal organisation may be very important in the fight against organised crime.

The Court recognised that the use and assessment of electronic evidence in criminal proceedings may entail specific difficulties for judges, due to its complexity, which may affect the ability of national courts to decide on its authenticity, accuracy and integrity. It also stated that, in criminal proceedings, national courts may increasingly rely on electronic data or other data gathered by intelligence services, whose activities in this respect may or may not be subject to the rules governing the obtaining of evidence within criminal proceedings.[23]

The ECtHR also held, however, that the right of access to the sources of evidence — and therefore the right to comment effectively on them — is not an absolute right and may be subject to limitations.[24] Therefore, it took into consideration whether the applicant's lack of access to the sources of evidence had been counterbalanced by adequate procedural safeguards and whether he had been given a proper opportunity to prepare his defence.[25] It is important to emphasise that the ECtHR does not call into question the use of intelligence information as evidence, leaving this matter to national legislation.

2. The bulk interception of communications and the *EncroChat* case at the CJEU

In the field of transnational evidence gathering and the admissibility of evidence obtained through the bulk interception of communications in the European Union (EU), perhaps no case has had greater resonance as the *EncroChat* case, on which the CJEU ruled on 30 April 2024.[26]

To briefly recall the facts of the case:[27] In the context of an investigation conducted by French law enforcement authorities, it emerged that some individuals under criminal investigation were using encrypted mobile phones operating under a licence called "EncroChat". The Lille magistrate authorised the use of a "Trojan horse" to access the entire messaging platform Specifically, the initial partial decryption of 3477 text files created as "notes" revealed that almost all of them were related to communications connected with criminal activities perpetrated by criminal organisations. The intercepted material was then distributed among the Member States for use in their own criminal investigations.

I will consider the case as establishing certain principles to be observed with regard to procedural safeguards in

criminal proceedings having a transnational dimension and involving electronic data and access to encrypted communication platforms in the Union.[28]

It may be argued that, strictly speaking, the case did not involve bulk surveillance, since access to the encrypted data was not carried out under a national security or intelligence scheme. Accessing the communications of users of the platform against whom no prior suspicion had been established, however, allows us to draw analogies with surveillance measures for preventive purposes and to approach the *Encrochat* case as if it were another bulk interception of communications. In this context, the CJEU had to deal with an unprecedented issue as to the use of non-targeted accessed communications as evidence in criminal proceedings and the rights of defence in cross-border digital environments.

Here, the Court in Luxembourg followed the criterion already adopted in the Strasbourg Court's case law[29] as well as in its own case law on data retention,[30] holding as follows:[31]

> As regards specifically the right to a fair trial, it must be noted in particular that if a court takes the view that a party is not in a position to comment effectively on a piece of evidence that is likely to have a preponderant influence on the findings of fact, that court must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an Infringement.

Interestingly, while the CJEU mentioned the lack of specific knowledge in digital matters on the part of the trial court as a factor to be taken into account when assessing defence rights in data retention case law, this was omitted in the ruling in the *EncroChat* judgment. Nevertheless, in defining the defence rights, the CJEU goes beyond the standards set out by the ECtHR in the *ByLock* case, in which the latter held that the right to comment effectively on digital evidence is not absolute. Furthermore, the CJEU ruled on the admissibility of evidence, by contrast to the ECtHR, which does not enter into establishing exclusionary rules of evidence, but analyses the case mainly from the fair trial rights' perspective (see also above 1.).

It remains to be seen how national courts interpret this rationale for inadmissibility of evidence, as defined by the CJEU. In the context of electronic evidence, the rights of the defence revolve around the ability to verify the lawfulness, authenticity, integrity, and proportionality of the evidence.

It follows that several questions arise: How can the integrity of the data be verified if access to the data in its entirety is not possible? Would the right to comment effectively imply a right of access to the raw data? How can the defence comment on bulk electronic data if sophisticated software is required to do so? Should data sifting always be done in the presence of the defence, as it is required for the cross-examination of witnesses? Does the state have to inform the defence about which AI tool was used to collect, process, and filter data?[32] Is there a need in the areas of freedom, security and justice for the EU Member States to always use a certified AI system? Should this be the same in all Member States?

3. Interim conclusion

As can be seen, both the ECtHR's case law and the CJEU's decision in *Encrochat* have already established a number of standards regarding bulk surveillance and bulk access to data. However, neither has defined which information gathered in this way can be used in criminal proceedings. While ECtHR and CJEU case law provide some guidance on the use of bulk surveillance and emphasise the need to ensure fair trial rights when encrypted messaging platforms are accessed, they do not prevent bulk data intercepted without prior identification of a suspect from flowing into criminal proceedings. On the one hand, the ECtHR expressly refrains from setting any standards on the admissibility of evidence in this context; on the other hand, the CJEU only establishes the need to ensure the possibility of "effective comment" on evidence obtained from a "suspected" platform. The question is whether these general standards are sufficient to ensure, in a digital context, not only the protection of privacy rights, but also that information gathered for preventive purposes and/or without suspicion does not become incriminating evidence. Should procedural safeguards be activated earlier, given that the rules on evidence seem to offer only limited protection against state interference in individuals' privacy rights via bulk surveillance?

III. Prevention, Mass Surveillance, and Open Data Analysis: The Challenges for Criminal Proceedings

The gathering and processing of information for security purposes (what is usually understood as intelligence) is not only a necessary and useful task but also indispensable if action is to be taken effectively against criminal phenomena in general, and organised crime, terrorism, money laundering, and environmental crime in particular.[33] However, given the scale of information gathering and the technological possibilities of mass surveillance, we should question whether an alternative or additional system for the prevention and/or prosecution of crime is being introduced surreptitiously, permeating procedural structures without an adequate and transparent legal framework and effective procedural safeguards.1. "Persons of interest" and the changing rules of the game to open criminal proceedings.

As has been widely pointed out, the boundaries between prevention and repression have become increasingly blurred in many areas, especially, but not only, in the fields of terrorism and organised crime. The reason for this is because criminal law has increasingly moved from repression to prevention[34] on the one hand and, on the other, measures of administrative law tend to acquire a punitive character.[35] This impacts not only fundamental rights, but also the very conception of criminal proceedings. The use of extensive preventive measures[36] has also led to the emergence of a new category of individuals who are not classified as suspects for the purposes of criminal proceedings, but who are identified as "persons of interest" or "pre-suspects" by algorithm-based mass surveillance systems.[37]

Classifying individuals as "persons of interest" based on their potential risk of committing criminal offences and subjecting them to continuous surveillance not only turns them into sources of information but also into objects of evidence, insofar as the data obtained from surveillance could acquire evidential value. Bulk data analysis can be initiated without the need to establish specific suspicions against particular individuals before a judge.[38] In many cases, a mere risk assessment is sufficient, and this assessment is regularly carried out by means of an algorithm.[39] In short, law enforcement authorities can access or purchase data analyses from companies that have the appropriate software to draw up not only profiles of potential risks, but, in particular, also profiles of those persons who represent a risk or who may directly be classified as criminal suspects. Thus, automated suspicion algorithms (ASAs) have come to increasingly replace informants and traditional police surveillance, while multiplying their reach exponentially. However, judges who must assess suspicions based on those ASAs within the criminal proceedings do not have clear criteria for determining their reliability.[40]

The consequence of all this is that the prerequisites for opening a criminal investigation may be completely altered by the new "rules of the game", because a thorough risk assessment can be carried out through the bulk analysis of data. This would then underpin the standard of probable cause required to open criminal proceedings. In short, it is worrying that an intrusive investigation can be initiated on the basis of the bulk processing of data for security purposes, without prior suspicion, since these surveillance measures only concern "persons of interest."[41] The joint, concurring opinion in *Big Brother Watch* (II.1.a above) indirectly pointed out this risk, which is dramatically increased by the AI development.

I neither contend that this is generally the case, nor that law enforcement or intelligence services are acting outside the law. However, even if we accept this premise and that these activities are carried out within legal limits — and I am not aware of any data contradicting this —, the truth is that any surveillance system lacking transparency and not being public must be subject to a rigorous oversight. It must be borne in mind that the bulk interception of communications and the retention of the data thus obtained constitute a significant interference with the right to privacy, even when the data are in fact not analysed.[42] Naturally, the risks are even greater when certain persons become surveillance targets owing to the selectors applied and the content of their communications is monitored and analysed. In *Big Brother Watch,* the ECtHR underlined the importance of oversight at all stages of the "surveillance procedure" (end-to-end safeguards), specifically highlighting oversight in the application of selectors (see II.1.a above).

The usefulness of bulk interception for security operations is scarcely disputed, and a proactive approach towards identifying threats to national security is regarded as a legitimate and reasonable aim. There are, however, two basic elements that clearly differentiate the levels of safeguards in criminal proceedings and in the preventive system aimed at security: In the field of criminal proceedings, there exists the requirement of prior suspicion and, usually, of a judicial warrant before investigative measures entailing an intrusion into fundamental rights can be taken; this warrant includes prior checking of the necessity and proportionality of the interference. In the case of non-targeted surveillance, the approach differs from the aforementioned criminal procedure scheme, since there is no initial judicial decision based on prior suspicions against specific individuals, simply because there is no specific target or suspect.[43] The risk of circumventing the safeguards of criminal proceedings seems to be clear.

While the case law of the ECtHR stresses the importance of oversight at all stages, it does not prevent the information gathered for security purposes to flow into criminal proceedings. Yet, the CJEU does not ban access to large amounts of data without prior suspicion against an identified suspect, as seen in the *Encrochat* case. This shows that, even if we can already count on a number of standards from the ECtHR and CJEU, the issue of implementing procedural safeguards in a digitalised surveillance environment has not yet been addressed.

2. Mass surveillance and criminal evidence standard

It could be argued that mass surveillance is not intended to gather evidence for criminal investigation purposes, since its focus is on prevention. But does this mean that the prin-

ciple of respect for privacy does not apply? If these data are the basis for obtaining evidence (having established a "reasonable suspicion" for a judicial warrant in order to initiate investigative measures), as outlined under 1. above, are we not caught in a vicious circle?

The fact that certain countries already use ASAs underpins these risks. As a result, criminal proceedings are no longer the place where facts and criminal liability are established, because, according to the algorithm used, data have already been collected against a "person of interest" and the next step is merely to present this data set as evidence. The evidence then secures the criminal conviction of an individual or, as a simpler solution, a plea agreement.[44] This phenomenon can be observed in criminal justice systems in which trials are slowly losing their previous importance and becoming the exception rather than the rule.[45]

This handling of evidence necessitates reconsideration of the system of procedural safeguards centered on the liberal model and, specifically, on the principle of a public and oral trial hearings, i.e., the moment at which adversarial proceedings reach their fullest expression in the taking of evidence. In order to solve the problem of using data from bulk interceptions as criminal evidence, the correct approach should be to reinforce the safeguarding prerequisites that may give rise to the opening of a criminal investigation against a specific person in the first place. We should rethink the role of "rational indications," "well-grounded suspicions," or "probable cause" (the term used in the Fourth Amendment of the United States Constitution).[46] Indeed, the term "probable cause" is ambiguous and as yet undefined, referring to a calculation of probabilities/to a non-quantitative or statistical probability that moves within a variable range.

The requirement of probable cause should become the decisive criterion when authorising access to and seizure of electronic data. In this context, it should not be overlooked, however, that the activation of an algorithm to identify or compile data by means of bulk processing could generate indications or suspicion criteria in respect of practically any individual. This could mitigate the normative and conceptual uncertainty of the probable cause standard and serve as the basis for initiating criminal proceedings, as well as for adopting criminal investigative measures that restrict fundamental rights (though they must still be subject to the additional criteria of necessity, suitability and proportionality).

In other words, if we wish to continue maintaining the traditional safeguards of criminal proceedings, the standard for activating investigative measures based on the processing of big data or for indiscriminately accessing retained user data, must be strengthened. It is worth noting here that the standard of probable cause "may not ultimately address any one right specifically, but instead protect all of liberty generally,"[47] thus safeguarding the rule of law principle.

We could still hope that the exclusionary rule of evidence would apply to data obtained prior to criminal proceedings or that evidence obtained solely on the basis of "reasonable suspicion" arising from mass surveillance would be declared invalid. This would be the procedural safeguard that governs the use of bulk data as evidence in criminal proceedings. However, this approach cannot be taken for granted, because the risk entailed is that it would suffice to confront the accused with all the data available to the prosecution to persuade the defendant to accept the conviction upon a plea agreement, without validity of the evidence never being assessed at trial.

IV. Concluding Remarks

A number of conclusions can be drawn from the discussion of the above-mentioned challenges:

Firstly, and perhaps most importantly, there is a need to continue the struggle for procedural safeguards in a digitalised world. Secondly, the prerequisites that allow the state to access and process citizens' data for preventive purposes need to be redefined. Thirdly, stricter control is also required over the application of the probable cause or "reasonable suspicion" requirement, as it could become the only way to prevent a criminal investigation from being opened and, subsequently, from turning any data already obtained into incriminating evidence. In a system that is primarily focused on prevention and technology, the defence can only assert its right to "comment effectively" on the evidence thus obtained.[48]

As the ECtHR held in *ByLock,* the right to effectively respond to the evidence obtained does not, however, necessarily include the right to review the integrity of the intercepted data or to have knowledge of the software used to access the communications. Any effort to strengthen the rights of the defence must include effective access to digital tools (knowledge of how the data was processed) and appropriate software (ability to analyse the raw data) in order to ensure the equality of arms. Otherwise, it will be impossible to comply with the adversarial principle as means of establishing facts in criminal proceedings.[49]

In any event, requiring prior suspicion as a prerequisite for taking notably intrusive measures into the citizens' sphere of privacy does not appear to protect us against mass surveillance. This became readily apparent in the *EncroChat* case at the level of the European Union, when national courts in the Member States accepted the intercepted communications as evidence against individuals despite there being no prior grounds for suspicion. It might be considered to revisit the standard of probable cause against the new digital reality and the resorting to data brokers for establishing automated suspicion algorithms.

In the EU, some progress has been made in protecting the rights of individuals facing criminal proceedings. The procedural rights directives adopted so far indicate that the European legislature has taken an increasingly progressive interest in establishing a framework of procedural safeguards. Yet, we must press on, as artificial intelligence and, in the near future, quantum computing usher in a new digital reality, bringing with it new challenges for criminal procedure. The time is ripe to articulate a new framework of procedural safeguards at the European level to cope with the increasing digitalisation of law enforcement.

* The present article was written within the framework of the research project NEO-TRANSCRIM: Criminal Evidence and New Challenges in Transnational Criminal Proceedings (PID2023-148413NB-I00), Spanish Ministry of Science, Innovation and Universities.

Prof. Dr. Lorena Bachmaier Winter
Full Professor of Law, Complutense University Madrid (UCM), Spain

1 See Bachmaier, "La lucha por las garantías procesales y el cambio de paradigma en materia de prueba: del proceso penal liberal a la mass surveillance", in L. Bachmaier Winter (ed.), *Prueba penal y derecho de defensa en la era digital. Nuevos paradigmas y nuevos retos,* Aranzadi, Cizur Menor, 2024, pp. 21–64.

2 See P. Galison & M. Minow, "Our Privacy, Ourselves in the Age of Technological Intrusions", in R. Ashby Wilson (ed.), *Human Rights in the «War on Terror»,* 2005, p. 260. More recently, on the use of AI in this field, see A. Sachoulidou, "Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence", (2023) *Artificial Intelligence and Law*, <https://doi.org/10.1007/s10506-023-09347-w>. All hyperlinks in this article were last accessed on 17 August 2026.

3 S. Brayne, *Predict and Surveil. Data Discretion and the Future of Policing*, 2020, pp. 122 ff. And, as R. Poscher, Guest editorial, *eucrim* 4/2025, 249 points out, this also requires a "re-calibration of traditional proportionality models" in digital-based surveillance.

4 The role of big tech corporations as necessary partners in the criminal investigation will not be further addressed here. See, in this regard, D. Bilchitz, "The Right to Privacy, Surveillance and the Global Obligations of Corporations", in D. Cole, F. Fabbrini and S. Schulhofer (eds.), *Surveillance, Privacy and Trans-Atlantic Relations*, 2017, pp. 113–136.

5 ECtHR, 6 September 1978, *Klass and Others v. Germany,* Appl. no. 5029/71.

6 ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* Appl. no. 37138/14.

7 ECtHR, 29 June 2006, *Weber and Saravia v. Germany*, inadmissibility decision, Appl. no. 54934/00.

8 ECtHR, 5 October 2006, *Zakharov v. Russia,* Appl. no. 14881/03.

9 ECtHR, 13 September 2018, *Big Brother Watch and others v. United Kingdom*, Appl. nos. 58170/13, 62322/14 y 24960/15; and later the *Grand Chamber* judgment of 25 May 2021. On this case, see L. Bachmaier Winter, "Proportionality, surveillance and criminal investigation: Strasbourg Court facing *Big Brother*", in E. Billis, N. Knust and J. P. Rui (eds.), *The Principle of Proportionality in Crime Control and Criminal Justice*, 2021, pp. 317–335.

10 There is a pending case seeking, once again, compliance with the Convention of the UK Investigatory Powers Act and addressing complaints about bulk interception warrants: ECtHR, *The National Council for Civil Liberties v. the United Kingdom*, Appl. no. 15250/24, lodged on 28 May 2024, published on 30 March 2026.

11 ECtHR (GC), 25 May 2021, *Big Brother Watch and others v. United Kingdom*, *op. cit.* (n. 9), para. 334.

12 Ibid., paras. 341–342.

13 Ibid., para. 348.

14 Ibid., para. 350.

15 Ibid., para. 354.

16 See the joint, partly concurring opinion of judges Lemmens, Vehabović and Bošnjak, para. 29.

17 ECtHR, 11 January 2022, *Ekimdzhiev and Others v. Bulgaria*, Appl. no. 70078/12.

18 ECtHR, 23 June 2022, *Haščák v. Slovakia*, Appl. no. 58359/12 *et al.;* See also ECtHR, 20 July 2021, *Zoltán Varga v. Slovakia,* Appl. no. 58361/12.

19 ECtHR, 28 May 2024, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, Appl. nos. 72038/17 and 25237/18.

20 ECtHR, 26 September 2023, *Yüksel Yalçinkaya v. Turkiye,* Appl. no. 15669/20.

21 Ibid., paras. 262–266, in which the ECtHR determines that the use of the encrypted platform is not sufficient evidence for the crime of membership of a terrorist organisation, as such an interpretation would run counter to Art. 7 ECHR.

22 Ibid. para. 312; see also 344.

23 Ibid., para. 312.

24 Ibid., para. 329.

25 Ibid., para. 330.

26 CJEU, 30 April 2024, Case C-670/22, *Criminal proceedings against M.N.* (*EncroChat*), ECLI:EU:C:2024:372.

27 The concrete events have still not been fully clarified. I refer here to the CJEU's judgment (*op. cit.,* n. 26), para. 19.

28 I will neither examine all aspects and implications of the communications data obtained through access to an encrypted system

used primarily for exchanging messages, nor all the questions revolving around the interpretation of the EIO Directive. I refer here to the vast literature on this case. See, e.g., T. Wahl, "Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren", (2021) 7–8 *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 453; J.J. Oerlemann and D. A. G. Van Toor, "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", *European Journal of Crime, Criminal Law and Criminal Justice, (*2022) 30(3–4), 309–328; L. Bachmaier, *op. cit.* (n. 1), 41. More recently, M. Lassalle and S. Lannier, "EncroChat – A Judicial Chronology. Interpretations from Paris, Strasbourg and Luxembourg Courts", (2025) 20 *eucrim*, 292–302.

29 ECtHR, 10 March 2009, *Bykov v. Russia*, Appl. no. 4378/02, paras. 88–90; ECtHR, 26 July 2011, *Huseyn and Others v. Azerbaijan*, Appl. nos. 35485/05, 45553/05, 35680/05, and 36085/05, paras. 199, 200, and 211; ECtHR [GC], 18 December 2018, *Murtazaliyeva v. Russia,* Appl. no. 36658/05; ECtHR, 14 February 2019, *SA-Capital Oy v. Finlandia*, Appl. no. 5556/10, para. 78; ECtHR, 14 March 2019, *Kobiashvili v. Georgia*, Appl. no. 36416/06, para. 56.

30 See, *inter alia*: CJEU, 17 December 2015, Case C-419/14, *WebMindLicenses*, ECLI:EU:C:2015:832; CJEU, 2 March 2021, Case C-746/18, *Criminal proceedings against H.K (Prokuratuur),* ECLI:EU:C:2021:152; CJEU, 30 April 2024, Case C-470/21, *La Quadrature du Net and Others v. Premier Ministre and Ministre de la Culture ('La Quadrature du Net 'II"),* ECLI:EU:C:2024:370.

31 CJEU, *EncroChat*, *op. cit.* (n. 26), para. 105.

32 On the problematics of AI evidence, see P.W. Grimm, M.R. Grossman and G.V. Cormack, "Artificial Intelligence as Evidence", 19 (2021) *Northwestern Journal of Technology and Intellectual Property*, 9. See also, in the EU context, the comparative study by K. Ligeti (ed.) *Artificial Intelligence as Evidence in Criminal Proceedings*, 2025.

33 See ECtHR [GC], 25 May 2021, *Big Brother Watch, op. cit.* (n. 9), para. 421; L. Bachmaier Winter, "Información de inteligencia y proceso penal", in L. Bachmaier (ed.), *Terrorismo, proceso penal y derechos,* Marcial Pons, Madrid, 2012, pp. 45–101, 49.

34 E.g., U. Sieber, "Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten", (2009) *Neue Zeitschrift für Strafrecht (NStZ)*, 353–364; U. Sieber, "Risk prevention by means of criminal law – On the legitimacy of anticipatory offenses in Germany's recently enacted counter-terrorism law", in F. Galli and A. Weyembergh (eds.), *EU counter-terrorism offences: What impact on national legislation and case-law?*, 2012, pp. 251–279; M.F.H. Hirsch, *Anticipative Criminal Investigation. Theory and Counter-terrorism Practice in The Netherlands and in the United States,* 2012.

35 L. Bachmaier, "The shift from criminal to administrative sanctions: the quest for fair trial rights in new crime control scenarios in the ECtHR case law", in M. Donini and L. Foffani (eds.), *La "materia penale" tra diritto naeionale ed europeo*, 2018, pp. 37–62; F. Galli, "The freezing of terrorists' assets: preventive purposes with a punitive effect", in F. Galli and A. Weyembergh (eds.), *Do labels still matter?,* 2014, pp. 43–68.

36 See A. Ashworth and L. Zedner, *Preventive Justice*, 2014, pp. 181–190.

37 I already analysed the situation of the pre-suspects or persons of interest in L. Bachmaier Winter, "Countering Terrorism: Suspects without Suspicion and (Pre-)Suspects under Surveillance", in: U. Sieber, V. Mitsilegas, C.C. Mylōnopulos, E. Billis, & N. Knust (eds.), *Alternative systems of crime control: national, transnational, and international dimensions*, 2018, pp. 171–191. I refer to the literature cited there.

38 M. Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment", (2016) 164 *Univ. Pennsylvania Law Rev.*, 870–929.

39 See Brayne, *op. cit.* (n. 3), pp. 118 ff.

40 L. Bachmaier (2024), *op. cit.* (n. 1), p. 42.

41 Ibid., 55.

42 As stated by the CJEU [GC], 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland et al*. para. 34. See also, on the chilling effect upon the rights of citizens and the impact upon the rule of law, D. Murray and P. Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data", (2019) 52 *Israel Law Review,* 31–60, at 43–47.

43 ECtHR [GC], 25 May 2021, *Big Brother Watch, op. cit.* (n. 9), para. 317. Nevertheless, in ECtHR, 28 April 2026, *Kanev and Bulgarian Helsinki Committee v. Bulgaria*, Appl. no. 45864/22, a case that concerned mass interception of communications by the intelligence services targeting numerous individuals in Bulgaria, the Court referred to the safeguards set out in *Big Brother Watch* (paras. 240–243). However, this case dealt with the agency's denial of information on the surveillance carried out.

44 See R. Lippke, "Plea Bargaining, Principled Sentencing, and Artificial Intelligence", in J. Ryberg and J.V. Roberts (eds.), *Sentencing and Artificial Intelligence*, 2022, 184–204.

45 See, e.g., Fair Trials, *The Disappearing Trial – What does justice mean in a world with more guilty pleas and fewer trials?*, 2017, <https://www.fairtrials.org/app/uploads/2022/01/The-Disappearing-Trial-Summary-Document-SF.pdf>.

46 See L. Bachmaier "Probable cause y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria", *Quaestio Facti*, vol. 4, 1/2023, 191–220, <https://revistes.udg.edu/quaestio-facti/article/view/22858/26542>.

47 B.A. Antkowiak, "Saving Probable Cause*", (*2007) 40(3) *Suffolk University Law Review*, 578.

48 As held in the CJEU *Encrochat* judgment (*op. cit.*, n. 26), para. 105 and the ECtHR *ByLock* case (*op. cit.,* n. 20), para.312.

49 As we proposed in Art. 7(5), of the ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU-.pdf>. This is also implicitly suggested in the judgement of the ECtHR, 4 June 2019, *Sigurður Einarsson and Others v. Iceland*, Appl. no. 39757/15; see also the dissenting opinion of judge *Pavli* there.

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

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 Pingen, 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, Head of Section (Antifraud Criminal Policy), 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: Stückle 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, 2026. 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
For cancellations of the subscription, please write an e-mail to:
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

https://eucrim.eu/

MAX PLANCK INSTITUTE
FOR THE STUDY OF
CRIME, SECURITY AND LAW