eucrim
2019 / 1
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: Evidence Gathering – Current Legal Issues
Dossier particulier: Recueil de preuves – questions juridiques actuelles
Schwerpunktthema: Beweissammlung – Aktuelle Rechtsfragen

2019/1 ISSUE / ÉDITION / AUSGABE

The Associations for European Criminal Law and the Protection of Financial Interests of the EU is 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. Joint seminars, joint research projects and annual meetings of the associations' presidents are organised to achieve this aim.

Contents

News*

European Union

Council of Europe

Articles

Evidence Gathering – Current Legal Issues

* The news contain Internet links referring to more detailed information. As of 2018, these links are being embedded into the news text. They can be easily accessed by clicking on the underlined text in the online version of the journal. If an external website features multiple languages, the Internet links generally refer to the English version. For other language versions, please navigate using the external website.

Guest Editorial

Dear Readers,

Twenty years have passed since the EU heads of state and government came together in Tampere and agreed that the principle of mutual recognition should become the cornerstone of judicial cooperation in criminal matters between the EU Member States. This was followed by the adoption of an ambitious list of mutual recognition instruments for the pre-trial, trial, and post-trial phases, which all reflect the same basic notions: direct contact between judicial authorities, uniform templates, short deadlines, a duty to recognise and execute (subject to limited grounds for refusal), and a presumption of mutual trust.

But what do twenty years of experience with the mutual recognition principle tell us? In the past two decades, judicial authorities have applied mutual recognition in practice when issuing and executing European Arrest Warrants (EAWs), European Investigation Orders (EIOs), and freezing, confiscation, and supervision orders. Despite its advantages, there ensued challenges and limits to this principle that were not always readily apparent. The authorities learned how differences between national legal systems complicate mutual recognition, but also how these differences can be overcome. The jurisprudence of the European Court of Justice (ECJ) provided insight into how key legal issues need to be interpreted in light of the mutual recognition principle.

There now exists a deeper understanding that mutual recognition is based on mutual trust, but not on blind trust. Often, additional information needs to be requested and there is a stronger awareness that mutual recognition is not only aimed at facilitating cooperation between authorities, but also at protecting individual rights. Perhaps most significantly, we have come to realise that mutual recognition is not a miracle solution. While it can be efficient and effective, it can also be cumbersome and complicated. Even though direct contact with colleagues abroad is a great starting point, it is not always sufficient. Fortunately, when judicial authorities need help in applying the principle of mutual recognition, they have Eurojust's support at their disposal.

Facilitating the execution of requests and decisions based on mutual recognition is at the heart of Eurojust's work. The number of EAW cases where Eurojust helped overcome practical and legal problems increased from 217 cases in 2013 to 410 newly registered cases in 2018. Particularly in recent years, ECJ case law raised new questions, and practitioners often struggled with requests for additional information and to meet deadlines. In 2018, Eurojust also opened 830 new cases on the EIO. The outcome report of the Eurojust Meeting on the EIO − summarized further on in this journal − provides a good overview of some of the main issues that mutual recognition has triggered. Similarly, the first preliminary ruling (Case C-324/17 *Gavanozov*) is currently pending before the ECJ and raises relevant questions on the meaning of mutual recognition and fundamental rights. It will be very interesting for practitioners to see how ECJ case law develops in the field of the EIO.

Ladislav Hamran

Applying the mutual recognition principle is not only about overcoming legal challenges. Efficient cooperation also requires judicial authorities to have the necessary practical means at their disposal, and a fundamental requirement for cross-border cooperation is a secure communication channel. Against this background, Eurojust recently launched an initiative to develop a digital infrastructure to support the exchange of operational information and evidence between judicial authorities across the EU, between judicial authorities and Eurojust, and between Eurojust and other JHA Agencies. This infrastructure will allow judicial authorities to identify connections between proceedings in different Member States more easily and to communicate more efficiently with Eurojust on cases requiring its support. Together with the secure online portal currently being developed by the Commission, I am convinced that it will soon greatly facilitate judicial cooperation.

Ladislav Hamran,
President of Eurojust

News

Actualités / Kurzmeldungen

European Union*

Reported by Thomas Wahl (TW) and Cornelia Riehle (CR)

Foundations

Fundamental Rights

EP: Potential of Charter Must Be Strengthened

The European Union must take resolute steps to strengthen its own engagements in guaranteeing the enjoyment of all of the rights of the Charter of Fundamental Rights, including social rights. This is one of the main requests of a EP resolution of 12 February 2019 "on the implementation of the Charter of Fundamental Rights of the European Union in the EU institutional framework." The non-legislative resolution was adopted by 349 to 157 votes (with 170 abstentions).

The resolution notes that there is a persistent awareness-gap concerning the Charter, its scope and degree of application among both rights-holders who benefit from its protection and legal and human rights experts. It also criticises that national action is scarce to remedy such a deficiency. The resolution addresses the importance of the Charter in the following matters:

- Strengthening the integration of the Charter in the legislative and decision-making processes;
- Mainstreaming the Charter into EU policies;
- The Charter and the EU Agencies;
- Implementation of the Charter at national level;
- More consistent interpretation of the Charter.

MEPs stress that the EU's legislative proposals must fully comply with the Charter; therefore, they advocate for enhanced forms of consultation, comprehensive impact assessments, and legal scrutiny with the involvement of independent experts in the field of fundamental rights. The EU's Fundamental Rights Agency should have a more vital role in the legislative process.

The resolution supports the introduction of strong and consistent fundamental rights clauses into the operational texts of the draft regulations establishing EU funds. It also calls on the EU institutions and bodies to make due regard to fundamental rights assessments if economic decisions are taken. Union's action on the international scene must be guided by the principles enshrined in Art. 21(1) TEU.

EU agencies operating in the sphere of justice and home affairs and/or those whose activities could have an impact on the rights and principles deriving from the Charter should adopt internal fundamental rights strategies and promote regular fundamental rights and Charter training sessions for their staff at all levels.

The Commission is called on to strengthen its awareness-raising activities concerning the Charter, with the full involvement of civil society organisations, and to promote and fund Charter-targeted training modules for national judges, legal practitioners as well as civil servants. In this context, the Commission should give full visibility to the FRA's recently published Handbook on Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level. Where needed, the Commission must safeguard fundamental rights through infringement proceedings.

Member States are encouraged to regularly exchange information and experience on the use, application and oversight of the Charter, and to mainstream the examples of best practice already developed at national level. Member States should also review their procedural rules on legal scrutiny and impact assessments of bills from the perspective of the Charter. (TW)

* If not stated otherwise, the news reported in the following sections cover the period 1 January – 31 May 2019.

EP: More Must Be Done for Effective Protection of Rule of Law and European Values

On 16 January 2019, the European Parliament called on all relevant actors at EU and national level, including governments, parliaments and the judiciary, to step up efforts to uphold and reinforce the rule of law.

The statement was made within a non-legislative resolution on the situation of fundamental rights in the European Union in 2017. The resolution was adopted with 390 votes to 153 and 63 abstentions.

Beside the rule of law, democracy, and fundamental rights, the resolution also addresses the following aspects:

- Right of migrants and refugees;
- Women's rights;
- Media freedom, freedom of expression and freedom of assembly;
- Racism, xenophobia, discrimination, hate speech and other forms of intolerance.

As regards the rule of law, MEPs condemn the efforts of some Member State governments to weaken the separation of powers and the independence of the judiciary. They express concern that – despite the fact that most Member States have adopted legislation to ensure judicial independence and impartiality, in compliance with Council of Europe standards – problems remain in the way these standards are applied, leaving national judiciaries open to political influence and fuelling public perceptions of interference in the judicial process and bias among individual judges. It is also pointed out that the separation of powers and the independence of the judiciary are essential to ensure the effective functioning of the rule of law in any society.

The EP recalls the need for an impartial and regular assessment of the situation with regard to the rule of law, democracy and fundamental rights in all the Member States. In this context, it reiterates the need for concluding a Union Pact for democracy, the rule of law and fundamental rights (EU Pact for DRF), as requested in two resolutions in 2016 and 2018 (cf. eucrim 3/2018, p. 144, and eucrim 4/2016, p. 154).

In the other areas, the resolution, inter alia, denounces the increasing restrictions to freedom of speech and freedom of assembly in the EU. It is also stressed that whistleblowing is crucial for investigative journalism and press freedom.

MEPs condemn the rise of far-right movements and trivialisation of hate speech. MEPs also point to abuses and human rights violations suffered by migrants and refugees in some Member States, in particular with regard to access to territory, reception conditions, asylum procedures, immigration detention and the protection of vulnerable persons. In the context of migration, the interoperability of large-scale information systems is acknowledged under the condition that it preserves the necessary safeguards.

Finally, the resolution recommends that the EU's Fundamental Rights Agency should be more involved if a legislative file raises serious fundamental rights issues. (TW)

Commission Triggers Debate on Future EU Rule-of-Law Toolbox

On 3 April 2019, the Commission published a Communication entitled "Further strengthening the Rule of Law within the Union." The Communication aims at triggering a reflection process on how the EU toolbox for defending and maintaining the fundamental value of the rule of law in the EU Member States can continue to be developed in the future. The Communication first recaps the core tools that the EU presently has at its disposal to ensure that the rule of law is upheld, e.g., the Rule of Law Framework (introduced in 2014), the Article 7 TEU procedure, infringement proceedings, the European Semester monitoring, and the EU Justice Scoreboard.

After assessing the experience made so far, the Communication lists three EU pillars to better enforce the rule of law in the Union:

- Promotion: This pillar involves building up knowledge and a "common rule of law culture;" it includes increased awareness raising in the general public and deepened cooperation with the Council of Europe.
- Prevention: The resilience of key systems and institutions must be built up by the EU, so that it is prepared when political stress arises. An in-depth understanding of the developments in the Member States is necessary for this purpose; areas of relevance include national checks and balances, judicial independence, the quality of public administration, anti-corruption policies, etc. In addition, extensive cooperation and dialogue can help resolve issues early on and foster reform processes.
- Response: If national rule-of-law safeguards are incapable of solving threats to the rule of law, it is the common responsibility of the EU institutions and Member States to take steps to remedy the situation. The Communication suggests a tailored approach. Actions may vary, depending on circumstances. One proposal is to cut EU money when rule-of-law deficiencies occur (see eucrim 1/2018, pp. 12–13). In addition, the 2014 Rule of Law Framework could be refined to include clear timelines for the length of dialogue.

The European Parliament, the Council, and other stakeholders have been asked to reflect on several questions with regard to each of the three pillars. The Commission will publish more conclusions and proposals at the end of June 2019. Additional background information on the rule-of-law process can be found on a special Commission website. (TW)

Romania to be Placed Under Rule-of-Law Monitoring

After Poland and Hungary, Romania is likely to become the third EU country that may face the consequences of the EU's Article 7 procedure (for this procedure, see eucrim 2/2018, p. 80 and the article by *Cassese*, eucrim 1/2018,

p. 72). After the Romanian Parliament passed a highly contentious justice reform on 24 April 2019, the Commission sent a warning letter to Romania on 10 May 2019.

The ruling Social Democrat party pushed the bill through in parliament, as a result of which the statute of limitations for some criminal offences is shorter, lower sentences for some offences have been introduced, and negligence in the workplace decriminalised. Critics believe that the reform *de facto* leads to impunity for high-ranking officials who are allegedly involved in corruption and fraud cases.

The Commission sees threats not only to judicial independence, but also to the effective fight against corruption, including the protection of the financial interests of the EU as a consequence of the new Romanian legislation. It warned the Romanian government that it will trigger the rule-of-law mechanism without delay and that it will suspend the Cooperation and Verification mechanism (CVM). The CVM is a specific framework for the Commission to regularly monitor progress made after Romania's accession to the EU in 2007. It was intended to help overcome several shortcomings that had been identified in relation to implementation of the EU *acquis*.

The Commission warned Romania that the country's envisaged accession to the Schengen area would be impeded if the controversial criminal law reforms are promulgated. (TW)

Council Does Not Reach Progress in Art. 7 TEU Procedure Against Poland and Hungary

At its meeting of 19 Feburary 2019, the General Affairs Council dealt with the Article 7 TEU procedure concerning Poland and Hungary. Statements of Member States on the rule of law situation in these two countries were, however, cautious. The Foreign Affairs Ministers of the EU Member States considered that recent legislative changes concerning the Supreme Court law in Poland were a positive development, but the Polish authorities are encouraged to address the remaining issues raised by the Commission.

The Article 7 procedure identifies a persistent breach of the EU's founding values by a Member States; it can lead to the suspension of certain rights of the Member State. The procedure against Poland was opened by the Commission on 20 December 2017. The procedure against Hungary was initiated by the European Parliament on 12 September 2018. Since then Council is dealing with matter, but – to date – without concrete results.

Furthermore, the Commission launched infringements proceedings against Poland before the CJEU because of the Polish Supreme Court's reform (see also eucrim 4/2018, 191 and 2/2018, 80). (TW)

AG: Polish Supreme Court Reform is Against EU Law

Polish legislation lowering the retirement age of Supreme Court judges violates EU law, according to the opinion of Advocate General *Evgeni Tanchev*. The opinion was released on 11 April 2019 and concerns one of three infringement procedures that have, in the meantime, been launched by the Commission against recent judicial reforms in Poland. The case is referred to as C-619/18. By order of 15 November 2018, the President of the Court granted the Commission's request to decide this action under an expedited procedure. On 17 December 2018, the CJEU already granted interim measures that, *inter alia*, obliged Poland to suspend application of its legislation on lowering the retirement age for Supreme Court judges (see eucrim 4/2018, 191).

In preparing the Court's final decision on the infringement action, AG *Tranchev* argued that the contested measures violate the principle of irremovability of judges, the observance of which is necessary to meet the requirements of effective judicial protection under the second subparagraph of Article 19(1) TEU. Irremovability, i.e., the protection of judges against removal from office, is one of the guarantees that is essential for judicial independence. The principle was violated in the given case because lowering the retirement age of Polish Supreme Court judges from 70 to 65 has a considerable impact on the composition of the Supreme Court (27 of 72 judges are affected), the measure is not temporary, and it applies retroactively. Societal and economic changes may justify adjustments to the retirement ages of judges, but they cannot compromise the independence and irremovability of judges.

In addition, the requirement of judicial independence was violated, because an extension of the mandate can only be granted by the Polish President, whose power to decide on extensions/renewals is inordinately broad. The extension decision is not subject to judicial review and is carried out without binding criteria, however, meaning that Supreme Court judges are exposed to external intervention and pressure from the President. This impairs the objective independence of the highest court and influences the judges' independent judgment and decisions. (TW)

Commission Launches Another Infringement Procedure Against Poland

The Commission has targeted another aspect of judicial reform in Poland. On 3 April 2019, the Commission launched a new infringement procedure against Poland. It addresses the recently introduced disciplinary regime for judges.

The Commission believes that the disciplinary regime is contrary to the obligations arising from Art. 19(1) TEUI in conjunction with Art. 47 CFR, which enshrine the right to an effective remedy before an independent and impartial court.

First, the new rules can subject ordinary court judges to disciplinary investigations, procedures, and, ultimately, to sanctions on account of the content of

their judicial decisions. Second, the newly created Disciplinary Chamber, which has been empowered to review decisions in disciplinary proceedings against judges, is not a court "established by law." Regarding the disciplinary proceedings, the Commission criticises the undue restriction of judges' procedural rights and the rights of the defence.

A second line of argumentation by the Commission involves non-compliance with Art. 267 TFEU – the right of courts to request preliminary rulings from the CJEU. According to the new disciplinary regime, judges may even face disciplinary proceedings for their decisions to refer questions to the European court.

Poland now has two months to react to the letter of formal notice in which the Commission opened the new infringement procedure.

This is the third infringement procedure against Poland. On 29 July 2017, the Commission launched an infringement procedure against the Polish Law on Ordinary Courts, on the grounds of its retirement provisions and their impact on the independence of the judiciary. The case was referred to the CJEU on 20 December 2017 (Case C-192/18).

On 2 July 2018, the Commission launched an infringement procedure against the Polish Law on the Supreme Court, on the grounds of its retirement provisions and their impact on the independence of the Supreme Court. The case was referred to the CJEU on 24 September 2018 (Case C-619/18). The CJEU granted the Commission's application on interim measures by order of 17 December 2018 (see eucrim 4/2018, 191).

In addition to the infringement procedures, the above-mentioned Article 7 procedure is still ongoing. It allows the Council to determine the clear risk of a serious breach of the rule of law by Poland. The procedure may end with the Council triggering a sanctioning mechanism: certain rights deriving from application of the EU treaties to the EU country in question may be suspended, including the voting rights of that country in the Council. (TW)

CCBE: Recommendations on Protection of Fundamental Rights in "National Security" Context

The concept of "national security" is often used in modern democratic societies to justify intrusive surveillance measures or other interference in an individual's fundamental rights. A universally accepted definition of national security is lacking, however, which makes it difficult for courts to review state actions by adequately applying the necessity and proportionality test. Therefore, the Council of Bars and Law Societies of Europe (CCBE) published a paper at the beginning of April 2019, which seeks to clarify the concept of "national security" as a justification ground. It also makes concrete recommendations as to how the invocation of national security by the executive can adhere to the rule of law. The paper is available in English and French.

After explaining the background and context of the subject matter and describing the existing legal instruments and case law at the European level, the paper presents the results of a survey conducted with a representative sample of members of bars and societies (Austria, Belgium, the Czech Republic, France, Germany, Greece, Hungary, Italy, Poland, Spain, and the United Kingdom). The survey included questions on the legal concept of national security, on how the concept is employed, on whether national security is defined in the law, and under what circumstances the term is invoked. The conclusion is drawn that the concept of "national security" is not precisely defined in most states' legal systems, but, when the state wishes to overcome legal restrictions, all legal systems use the concept.

Against this background, the following definition of national security is suggested: "(N)ational Security is understood as the internal and external security of the state, which consists of one or more of the following elements:

- the sovereignty of the state;
- the integrity of its territory, its institutions and its critical infrastructure;
- the protection of the democratic order of the state;
- the protection of its citizens and residents against serious threats to their life, health and human rights;
- the conduct and promotion of its foreign relations and commitment to the peaceful coexistence of nations."

The CCBE does not stop at the definition, however, but emphasises that "procedural justice" is also needed. This means that state authorities must heed rule-of-law principles if they invoke the rationale of "national security" and citizens must receive a clear and fair procedure in the event of infringements of their fundamental rights. In this context, the CCBE makes four recommendations:

- Need for legislative control;
- Judicial and independent oversight;
- Effective legal remedies and sanctions;
- Protection of the professional secrecy and legal professional privilege.

The CCBE concludes that its contribution is designed to enable "democratic societies (to) respond to internal and external threats (…), whilst yet upholding the democratic values on which they are founded." (TW)

Security Union

Commission Takes Stock of Security Union Progress

On 20 March 2019, the European Commission presented its 18th "progress report towards an effective and genuine Security Union." Within the framework of this series (see also eucrim 3/2016, 123), this report especially takes stock of the progress made on the main building blocks of the EU's Security Agenda – prior to the European Parliament (EP) elections in May 2019. The report also highlights the need for further action in the near future.

The report notes that 15 of 22 legislative priority files presented by the Commission have been agreed upon by the EP and the Council. These include restrictions on the marketing and use of explosives precursors and the interoperability of the EU information systems. Good progress has also been made on the Commission proposal to strengthen the security of identity cards and residence documents. The removal of terrorist content online (see eucrim 4/2018, 199) and the reform of the European Border and Coast Guard remain high on the legislative agenda.

Steady progress has also been made in building up electoral resilience. Measures include the introduction of stricter rules on political party funding. One important issue in the context of electoral resilience is the fight against disinformation. Here, the Commission points out a recently introduced Rapid Alert System and its regular monitoring of the code of practice against disinformation, which is implemented by online platforms, e.g., Google, Facebook, and Twitter. A specific progress report on the code of practice was published on 20 March 2019.

In the area of enhancing critical infrastructure, the Commission plans to concentrate on common security standards for 5G networks, which are set to become the backbone of future global telecommunications.

As regards the fight against terrorism, the Commission report stresses the enhanced security of public spaces, where a set of "good practice" has been established by the Commission in close cooperation with public authorities and private companies. Better support for victims of terrorism remains vital. The Commission plans to fund a new EU Centre of Expertise – a platform for practitioners dealing with victims of terrorism; the centre is to be established in 2019.

Lastly, the Commission emphasised that Internet security and cybercrime remains an area of concern. It refers to a Eurobarometer survey of March 2019 in which an increased number of Europeans expressed concern over falling victim to various forms of cybercrime. For example, seven in ten respondents fear become the victim of devices infected with malicious software, of identity theft, or of bank card/online banking fraud. (TW)

EP-Studies on Algorithmic Decision-Making

The European Parliamentary Research Service published two studies dealing with algorithms used in systems to support decision-making. The studies were designed to provide a basis for future debates in the European Parliament on the issue of algorithmic decision-making systems.

The first study, "Understanding algorithmic decision-making: Opportunities and challenges," focuses on the technical aspects of algorithmic decision systems (ADS) and explores the benefits and risks of ADS for individuals, for the public sector, and for the private sector. The study also includes examples of ADS in criminal justice, e.g., predictive policing, risk assessments for recidivism, and the use of ADS for sentencing. In conclusion, the study puts forward various options for policymakers and the public to address precautionary measures that meet the raised challenges. These options include:

- Developing and disseminating knowledge about ADS;
- Publicly debating the benefits and risks of ADS;
- Adapting legislation to enhance the accountability of ADS;
- Developing tools to enhance the accountability of ADS;
- Effectively validating and monitoring measures for ADS.

The second study develops policy options for a governance framework for algorithmic accountability and transparency. It analyses social, technological, and regulatory challenges posed by algorithmic systems. The study, *inter alia*, deals with algorithm-based decision-making in the US criminal justice system as an example of algorithmic fairness – in view of the authors, algorithmic fairness is a guiding principle for transparency and accountability.

As regards governance frameworks, the study explains a number of fundamental approaches to technology governance, provides a detailed analysis of several categories of governance options, and reviews specific proposals for the governance of algorithmic systems as discussed in the existing literature. The study breaks down the assessments into four policy options:

- Awareness raising: education, watchdogs, and whistleblowers;
- Accountability in public-sector use of algorithmic decision-making;
- Regulatory oversight and legal liability in the private sector;
- Global dimension of algorithmic governance.

Each option addresses a different aspect of algorithmic transparency and accountability and includes concrete recommendations for policy-makers. (TW)

EU Law Enforcement Emergency Response Protocol

In order to provide law enforcement authorities in the EU with a tool for immediate response to major cross-border cyber-attacks, the Council of the EU adopted an EU Law Enforcement Emergency Response Protocol. The Protocol, on which Europol reported in March 2019, is part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises of September 2017. It sets out a multi-stakeholder process with seven possible core stages beginning with the early detection and identification of a major cyber-attack. The next steps include threat classification, an emergency response coordination centre, early warning notification, a law enforcement operational action plan, investigation and multi-layered analysis, and ultimately, emergency response protocol closure.

The protocol determines the procedures, roles and responsibilities of key players both within the EU and beyond. It sets out secure communication channels and 24/7 contact points for the exchange of critical information; as well as the overall coordination and de-confliction mechanism.

The scope of the protocol only covers "cyber security events of a malicious and suspected criminal nature" and does not include incidents or crises caused by a natural disaster, man-made error or system failure. (CR)

Area of Freedom, Security and Justice

2019 EU Justice Scoreboard: Downward Trend for Judicial Independence

spot light

On 26 April 2019, the Commission published the 2019 EU Justice Scoreboard. The Scoreboard presents an annual comparative overview of indicators relevant for the independence, quality, and efficiency of justice (for the Justice Scoreboards of previous years, see eucrim 2/2018, 80–81, and eucrim 2/2017, 56). The parameters are an essential tool for measuring the effectiveness of national justice systems. The data are important for the EU – not only to lay the basis for good investments and to attract businesses, but also to monitor the rule-of-law value.

In general, the 2019 Scoreboard indicates positive trends as regards the efficiency of justice systems and the quality of justice:

➤ *Efficiency*

- In almost all EU Member States, the length of first-instance court proceedings remained stable or even decreased since 2010;
- Those Member States facing substantial challenges showed an increase in the length of proceedings in 2017;
- The length of proceedings specifically as regards money laundering cases varied: in approx. half of the Member States, they take up to one year on average; they take around two years on average in a number of other Member States.

➤ *Quality in terms of accessibility*

- Almost all EU Member States provide some online information on their judicial systems; however, differences remain as regards information content and adequacy for the people's needs;
- Over the years, legal aid for consumers has become less accessible in some EU Member States;
- In some Member States, there are dissuasive effects compromising access to justice for people in poverty.

➤ *Quality in terms of resources*

- Overall, in 2017, general government total expenditure on law courts remained mostly stable in Member States;
- In half of the Member States, over 50% of the judges regularly participate in continuous training measures on EU law or the law of another EU Member State;
- The percentage of regular training in other skills, such as judgecraft, IT, court management, and judicial ethics, remains very heterogeneous within the EU Member States.

➤ *Quality in terms of assessment tools*

- Several Member States extended monitoring to more specific elements and some involved more specialised court staff for quality compared to past years;
- Compared to previous years, there was no improvement in implementing ICT case management systems in many Member States;
- Surveys among court users and legal professionals have decreased, with more Member States opting not to conduct any surveys.

➤ *Quality in terms of setting standards*

- For the first time, the 2019 Justice Scoreboard includes data on standards regarding the quality of judgments. Standards vary considerably among the EU Member States, but most provide some kind of professional training for judges on the structure, style of reasoning, and drafting of judgments;
- As a good practice to improve citizen-friendly justice, access mechanisms have been put in place for court users to obtain clarification on court decisions. Only some EU Member States provide these mechanisms;
- Those Member States facing efficiency challenges are currently not using timing standards;
- Standards for backlogs are still not as widespread as those fixing time limits and timeframes;
- Only a few Member States have continuous monitoring mechanisms for predefined timeframes.

As regards the *independence of justice*, the Scoreboard mainly measures perceived independence by EU citizens and companies. Data are obtained by means of several surveys, conducted, e.g., by Eurobarometer and the World Economic Forum. The 2019 Justice Scoreboard concludes that, although the perception of judicial independence improved in about two-thirds of Member States compared to 2016, the perception of judicial independence by businesses and the general public decreased in about three fifths of all Member States compared to the 2017 Scoreboard. The most frequently stated reason for the perceived lack of independence of courts and judges is interference or pressure from government and politicians. The second most frequently stated reason is pressure from economic or other specific interests. Both reasons stated above are noteworthy for those Member States in which perceived judicial independence is very low.

For the first time, the 2019 EU Justice Scoreboard includes information on disciplinary regimes for judges in the various national systems. It also provides information on the appointment and dismissal of prosecutors. These data are important indicators for the independence of justice systems in the EU.

The EU Justice Scoreboards will also feed the so-called European Semester, where the European Commission carries out a detailed analysis of EU Mem-

ber States' plans for macroeconomic, budgetary, and structural reforms. It issues recommendations on a country-by-country basis for a period of 12–18 months to be adopted by the Council. If the results indicate poor performance in individual Member States, the Commission will take a closer look at their legislation and institutions. (TW)

Brexit: UK Government Prepares No Deal Scenario in the Areas of Security and Criminal Justice

The British government tabled "Regulations" that contain legislative amendments and regulatory measures in the area of security, law enforcement and criminal justice. They are to ensure that the UK's statute book continues to function effectively, should the UK leave the EU without an agreement in March 2019. The Regulations will address failures of retained EU law to operate effectively or address other legislative deficiencies arising from the UK's withdrawal from the EU. It is told that they "will provide legal and operational certainty."

The instrument deals with the whole array of security, law enforcement and criminal justice issues, such as:

- Counter-terrorism;
- Cross-border surveillance;
- Eurojust;
- Europol;
- European Judicial Network;
- ECRIS;
- Exchange of information and intelligence between law enforcement authorities and disclosure in foreign proceedings;
- Extradition;
- Mutual legal assistance in criminal matters;
- Joint Investigation Teams;
- Passenger name record data;
- Prüm cooperation;
- Schengen Information System;
- Proceeds of crime;
- Serious crime and fraud.

An Explanatory Memorandum explains topic by topic (1) what did any relevant EU law do before Brexit day, (2) why is it being changed, and (3) what will it now do. Further explanations on the legal context and policy background detail the impact of the regulations in case of "no deal" and give an overview of whether EU rules continue to apply or are to be revoked. This includes the fact that the UK will no longer be a party of Europol and Eurojust, for instance.

As regards extradition, the Regulations point out that they will provide the legislative underpinning for the UK to transition its cooperation with Member States to a non-EU mechanism. This means that the UK will no longer operate the European Arrest Warrant after Brexit end of March 2019 without a transitional agreement. Lawyer *Rebecca Niblock* from Kingsley Napley analysed the regulations in relation to extradition at the blog "Lexology." She argues that the chosen option of falling back to the 1957 European Convention on Extradition poses numerous problems. (TW)

Schengen

ETIAS Implementation: Progress by Frontex and Europol

At the beginning of May 2019, both Frontex and Europol submitted progress reports to the European Parliament and the Council of the EU on the preparatory status of the European Travel Information and Authorisation System (ETIAS). For the legal framework of ETIAS, see eucrim 2/2018, 82, 84.

According to Frontex, the Agency has already made the following preparations:

- Created a task force for management of the ETIAS and an interoperability programme;
- Analysed the relevant regulations to identify its detailed responsibilities;
- Contributed to the Commission's drafting of delegating acts and implementing decisions;
- Organised a high-level seminar for EU Member States.

Additional tasks for 2019 include further designing the operational model of the ETIAS Central Unit and establishing a recruitment plan for the Unit.

Europol has participated in implementation meetings and conducted an internal business analysis elaborating the operational processes in which it is expected to be involved. It has also already taken an initial technical step by making its data available for the European Search Portal and for the future cross-checking of ETIAS travel applications. (CR)

Legislation

Updated Rules on European Citizens' Initiatives

At the end of March 2019, the Council and the European Parliament passed a Regulation that reforms the European citizens' initiative. The European citizens' initiative is a democratic participation tool by which citizens may influence EU policy. If the Commission has the power to propose legislation, e.g., on the environment, transport, agriculture, energy, or trade, a successful initiative may demand the Commission to take legislative action. Supporters of an initiative must total at least one million and come from at least one quarter of EU Member States. The basic rules are laid down in a Regulation of 2011.

The new Regulation aims at making the European citizens' initiative more accessible, less burdensome, and easier to use. It introduces a central online system available to organisers free of charge. Support for an initiative can be provided electronically.

Assistance for organisers has been improved and the translation of all initiatives into all EU languages ensured. Support requirements have also been lowered, e.g., supporters can back initiatives regardless of their country of residence and fewer personal data need to be provided. Member States are encouraged to give young supporters more possibilities to participate, i.e., in accordance with their national laws, the minimum age for supporting an initiative may be set at 16 years.

In addition, the follow-up process for initiatives has been improved. One example is the extension of the examination period from 3 to 6 months, which ensures that there is enough time for EP hearings, Commission analyses, and other debates.

The new rules will apply as of 1 January 2020. (TW)

European Citizens' Initiative on Respect for the Rule of Law Admitted

On 3 April 2019, the Commission registered a European citizens' initiative called "Respect for the rule of law within the European Union."

The European citizens' initiative is a democratic participation tool by which citizens may influence EU policy. It was introduced by the Lisbon Treaty. If the Commission has the power to propose legislation, a successful initiative may demand that the Commission to take legislative action.

The "Rule of Law" initiative aims at creating "an objective and impartial evaluation mechanism to verify the application of the European Union's values by all the Member States." The Commission is called upon to "provide the European Union with general legislation […] to verify the practical application of national provisions relating to the rule of law." In addition, the organisers aim to "facilitate the enforcement of European laws on judicial cooperation in criminal matters (e.g. the European Arrest Warrant)" and to strengthen the role of the European Union Agency for Fundamental Rights.

The Commission held that all admissibility criteria had been fulfilled. In particular, the EU Treaties give the Commission the necessary legislative competences. The Commission is allowed to launch legislative proposals on evaluation of the Member States' implementation of Union policies in the area of freedom, security and justice. It may also draft laws on strengthening the European Union Agency for Fundamental Rights.

The organisers now have one year to collect 1 million statements of support from at least seven different Member States. If this is successful, the Commission must decide whether to follow the request or not. In either case, the Commission must provide a reasoning for its decision.

The initiative accompanies the Commission's Communication to reflect on future EU measures to ensure rule-of-law values, the Commission's decision to launch another infringement proceeding against Poland for not respecting the rule of law in its recent justice reform on disciplinary proceedings against judges, and the adoption of new, more user-friendly rules on European citizens' initiatives by the EP and the Council. (TW)

Roadmap Proposed for New Decision-Making Procedure in EU Tax Policy

On 15 January 2019, the European Commission kicked off a policy debate on reforming the EU's decision-making in taxation. This area is currently subject to a special legislative procedure, the Council being the sole legislator and deciding by unanimity. The European Parliament is consulted only, i.e., the Council is not legally obliged to take the Parliament's opinion into account.

The Commission's Communication "Towards a more efficient and democratic decision making in EU tax policy" (COM(2019) 8) lists the disadvantages of the current system and the advantages of a future qualified majority voting procedure (QMV) in the Council under the ordinary legislative procedure, i.e., the EP having an equal say alongside the Council.

In the past, unanimity created unnecessary delays and was a tool to obtain concessions. Often, objections by Member States' delegations were not related to the tax matter in question. This is apparent in the EU Savings Directive, for example, which took 26 years from proposal to adoption.

The Commission also demonstrates that a definitive VAT regime could also help stop carousel fraud and save the EU taxpayer €50 billion in losses per year. A more efficient tax policy would also increase annual revenues within the EU and enhance economic growth.

The Commission suggests a roadmap for a progressive and targeted transition to QMV under the ordinary legislative procedure in certain areas of shared EU taxation policy. This is considered necessary for the following reasons:

- Citizens demanding action;
- Improved cooperation;
- More democratic decision-making;
- Stronger Single Market;
- Fairer taxation;
- The EU becoming a global leader in a fairer tax environment.

The Commission suggests four steps for a fairer and more efficient taxation policy:

- *Step 1: combating tax evasion/fraud.* Member States would agree to move to QMV decision-making for measures that improve cooperation and mutual assistance between Member States in fighting tax fraud/tax evasion and for administrative initiatives for EU businesses, e.g., harmonised reporting obligations;
- *Step 2: tax as supporting policy in other areas*. QMV would be introduced to advance tax measures as a support tool for other policy goals, e.g., fighting climate change, protecting the environment, and improving public health;
- *Step 3: further harmonisation of tax policy.* QMV would be used to help modernise already harmonised EU rules, e.g., VAT and excise duty rules. Faster decision-making in these areas would allow Member States to keep up with the latest technological developments and market changes, which would benefit EU countries and businesses alike;
- *Step 4: tax initiatives necessary for Single Market.* A shift to QMV is envisaged for major tax projects, e.g., the Common Consolidated Corporate Tax Base (CCCTB) and a new system for taxation of the digital economy, which are urgently needed to ensure fair and competitive taxation in the EU.

The Commission suggests that decisions on Steps 1 and 2 should be taken

swiftly. Steps 3 and 4 should be developed by the end of 2025.

The Commission also stresses that its proposals entail neither a change of EU competencies nor of Treaty provisions. The shift to QMV and the ordinary legislative procedure is already allowed under certain circumstances by the so-called "passerelle clauses," e.g., Art. 48(7) TEU.

The Commission calls on EU Member States, the EP, and all stakeholders to engage constructively in a debate on QMV in EU tax policy. In particular, EU leaders are invited to endorse the proposed roadmap and to make timely decisions on use of the relevant legal provisions set out in the Treaties. (TW)

Record of Legal Practitioners' Trainings in 2017

In 2017, over 180,000 legal practitioners (judges, prosecutors, court staff, lawyers, bailiffs and notaries) took part in training activities on EU law or the law of another Member State. With this record number over all seven years since reporting on European judicial training since 2011, the EU reached its goal to let attend half of all legal practitioners in the EU (i.e. around 800,000) training by 2020. Hence, the target set in the European Judicial Training Strategy of 2011 has been achieved two years ahead of schedule.

This is the main result of the European Commission's report on training for EU legal practitioners in 2017, which was published end of December 2018.

According to the report, the 2017 figures show an upward trend in the numbers of practitioners trained on EU law. The participation rate varies, however, across the different legal professions and Member States. Whereas the degree of training remains stable for judges and prosecutors, there is more fluctuation for court staff, lawyers and notaries. The report contains detailed breakdowns. These include training participation by profession, length of training, training topics and quality indicators.

The absolute numbers of professionals trained have increased for all professions (except bailiffs). Judges and prosecutors received far more training on EU law or the national law of another Member State than members of the other professions.

In most Member States that delivered data, the total number of lawyers trained increased. The report states, however, that the situation of lawyers' trainings remains widely unsatisfactory.

It should be noted that the figures are meaningful to a limited extent only, since data are not or not fully provided by all Member States and data on private providers of training for lawyers are lacking.

The report concludes that there is still room for improvement. The Commission is set to present a robust evaluation of the 2011 strategy and bring forth recommendations for the future in 2019. For the debate on the rehaul of the training strategy, see also eucrim 1/2018, 4–5.

All reports on European judicial training can be consulted via the EU's e-justice portal. (TW)

Institutions

European Court of Justice (ECJ)

New Rules for Repetitive Appeals

With effect from 1 May 2019, the Protocol on the Statute of the Court of Justice of the European Union and the Rules of Procedure of the Court of Justice have created new rules for appeals brought in cases that have already been considered twice - initially by an independent board of appeal, then by the General Court. Under the new procedure, the Court of Justice will now only allow an appeal to proceed, wholly or in part, if it raises a significant issue with respect to the unity, consistency, or development of EU law. In concrete terms, an appeal brought against a decision of the General Court on a decision of an independent board of appeal of one of the following will not proceed unless the Court of Justice first decides that it should be allowed:

- The European Union Intellectual Property Office (EUIPO);
- The Community Plant Variety Office (CPVO);
- The European Chemicals Agency (ECHA);
- The European Union Aviation Safety Agency (EASA).

To be admissible, such appeals must now be accompanied by a request clearly setting out the significant issue raised by the appeal with respect to the unity, consistency, or development of EU law. (CR)

Record Number of Cases in 2018

According to its judicial statistics for the year 2018, the Court of Justice and the General Court completed a record number of 1769 cases in 2018 – this marked a new record in the courts' productivity. The previous two years had seen approx. 1600 completed cases per annum. In addition, the number of pending cases also dropped to 2334 cases in 2018 compared to 2420 in 2017.

At the same time, the number of cases brought before the Court of Justice once again increased in 2018, with 849 new cases representing an increase of 15% compared to 2017. The majority of these cases were references for preliminary rulings, with 568 requests representing 70% of the cases pending before the Court of Justice. As regards the processing time for references for a preliminary ruling, statistics indicate a slight increase from 15.7 months to 16 months in 2018. (CR)

OLAF

Investment Fund Misuse in Romania

On 9 April 2019, OLAF reported on a successful operation led by the Romanian National Anti-Corruption Directorate

(DNA). With OLAF's support, investigators revealed a kickback scheme being used by an organised criminal group that involved corruption, influence peddling, and money laundering. Losses in EU investment funds amounted to over €2 million. Eurojust financially supported the operation activities of the Joint Investigation Team. (TW)

International Operation Against Fake Shampoo

On 18 February 2019, OLAF reported a successful international operation which searched and seized 400 tons of counterfeit shampoo having an estimated retail value of €5 million. The fake haircare products stem from China and were shipped over different ports in China and Korea to Latin America. OLAF was able to keep track on the shipment with special software. With OLAF's coordination and the support of the Spanish customs service, the Columbian and Mexican authorities stopped the cargo before it could reach its end destination in Venezuela where the products were to be distributed. Hence, import into the European market could be prevented.

OLAF stressed that the trade with counterfeit products not only leads to significant losses of tax revenue. The smuggling of counterfeit products also harms the European economy, damages legitimate business and stifles innovation, putting many jobs at risk. Counterfeiting also poses serious risks to health and safety as well as the environment. (TW)

Eurojust

Eurojust Annual Report 2018

At the beginning of April 2019, Eurojust published its Annual Report for the year 2018.

In 2018, Eurojust once again saw an increase in its casework, with 3317 new cases. The majority of cases dealt with fraud (907), drug trafficking (451), and money laundering (432). 545 of these cases also involved third states. In total, Eurojust dealt with over 6500 cases in 2018, the largest number in its history. Furthermore, 85 new Joint Investigation Teams (JITs) were signed off in 2018.

'Operation Pollino' serves as an example of a major organised crime investigation that was conducted in 2018 and shows how Eurojust works.

Looking at priority areas such as counter-terrorism, cybercrime, and migrant smuggling, Eurojust worked on 191 terrorism cases, 219 cybercrime cases, and 157 migrant smuggling cases in these areas. 28 coordination meetings were organised at Eurojust on cybercrime cases alone. In the area of counter-terrorism, 2018 saw a proposal to set up a European Judicial Counter-Terrorism Register at Eurojust, with the aim of detecting possible links between ongoing investigations conducted in different Member States and identifying the coordination needs between all judicial authorities concerned.

Developments with regard to Eurojust's cooperation with third States included the deployment of Liaison Officers of the Ukraine and North Macedonia at Eurojust. Contact points from Nigeria, Iran, Mauritius, and South Africa recently joined Eurojust's international judicial contact point network. Albania signed a cooperation agreement, and first steps were also taken to strengthen cooperation with Libya. Furthermore, negotiations for a cooperation agreement with Frontex were started.

Eurojust's support in the area of mutual recognition and the use of judicial cooperation tools in 2018 amounted to assistance in over 1000 European Investigation Orders and 700 European Arrest Warrants.

In 2018, Eurojust presented a general proposal on Digital Criminal Justice. The proposal aims at answering the need to keep pace with the growing interconnectivity and digitalisation of cooperation among law enforcement agencies in Europe.

Looking ahead, the new Eurojust Regulation will become applicable in December 2019, changing Eurojust from the European Union Judicial Cooperation Unit to the EU Agency for Criminal Justice Cooperation.

Lastly, the report is critical of the budgetary reductions foreseen for Eurojust in 2019 and to its Multi-Annual Financial Framework, which poses a real challenge for the Agency and its increasing number of cases.

Eurojust Newsletter Available

Eurojust has started to publish a quarterly newsletter outlining the Agency's recent work and latest publications.

The very first edition covers the period from January to March 2019, presenting the highlights of Eurojust's casework, articles, reports, and other published documents. It also covers key events during that period. The newsletter includes a brief outlook on the key developments to be expected in the second quarter. (CR)

Cooperation Between Eurojust and Georgia

On 29 March 2019, Eurojust and Georgia signed a cooperation agreement to strengthen their fight against cross-border organised crime.

The agreement allows for Eurojust and Georgia to exchange judicial information and personal data in criminal investigations and prosecutions across Europe and gives Georgia access to Eurojust's information systems. Furthermore, Georgia will be able to appoint a Liaison Officer to Eurojust.

The cooperation agreement is the first one signed between Eurojust and a State of the South Caucasus region. (CR)

New National Member for Latvia

On 1 May 2019, Ms *Dagmāra Skudra* took up her position as National Member for Latvia at Eurojust. She previously held the position of Deputy to the National Member of Latvia at Eurojust from 2004–2013.

Before joining Eurojust, Ms Skudra was Deputy Prosecutor General and Head Prosecutor of the Department of Analysis and Management with the Latvian Prosecutor General's Office. (CR)

New Eurojust National Member for Estonia

This March, a new National Member for Estonia, *Laura Vaik*, took office at Eurojust. Prior to her position as Estonian National Member, Ms Vaik served as State Prosecutor in the Prosecution Department and in the Internal Control Department of the Prosecutor's General Office of Estonia. During that time, she was already seconded as national expert to the Estonian Desk at Eurojust. (CR)

Eurojust/Europol Report on Encryption

On 11 January 2019, Eurojust and Europol published their first joint report on encryption offering an overview of the state of play in this area. Encryption is defined as the process of converting data, such as messages or pieces of information, in a way that prevents unauthorised access.

The report is primarily directed at policymakers. It gives an introduction to the basics of encryption, products and services using encryption, the encryption challenge for law enforcement and prosecution, and a look forward.

With regard to the basics of encryption, the report explains the differences between symmetric and asymmetric encryption as well as cryptographic hash functions.

Looking at products and services using encryption, it outlines the use of encryption in voice communications, full disk encryption, e-mails, file sharing, and self-destructing and anonymous applications.

Analysing the challenges for law enforcement and the prosecution reveals that it is becoming progressively more difficult for law enforcement to gain access to encrypted data in the context of investigations. Hence, the report offers insight into the advantages and disadvantages of a number of possible workarounds like guessing the key.

Ultimately, the report looks at possible future developments with respect to encryption, e.g., quantum computing, artificial intelligence, 5G communication technology, and steganography. (CR)

Second EuroMed Forum

From 30–31 January 2019, Prosecutors General from Europe and Mediterranean countries took part in the second EuroMED Forum of Prosecutors hosted by Eurojust in The Hague. This year's Forum dealt with issues such as the fight against terrorism and organised crime as well as personal data protection. Furthermore, members of the Forum agreed on guidelines for setting up the principles of collaboration, communication, and continuation of the Forum.

Among the Mediterranean countries represented were Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, the Palestinian National Authority, and Tunisia. (CR)

Europol

Cooperation with the European Merchant Risk Council

On 5 April 2019, Europol's EC3 and the European Merchant Risk Council (MRC Europe) signed a Memorandum of Understanding to combat serious organised crime, especially in the area of e-commerce fraud.

MRC is an independent, non-profit business association that promotes collaboration between eCommerce payment systems and risk professionals. It supports over 500 member companies, representing a variety of industries, technologies, services, and solutions. The focus is on optimizing payments and reducing eCommerce fraud. (CR)

Cooperation with Perseuss

On 28 February 2019, Europol signed a Memorandum of Understanding with Perseuss to enhance their efforts to combat online fraud. Perseuss is a global platform based on fraud records of merchants from across the globe who aim to share fraud intelligence. Europol and Perseuss have already successfully cooperated in operations such as the Global Airline Action Days (GAAD) where Perseuss assisted with the detection of airline fraudsters. (CR)

FinCEN Liaison Officer at Europol

On 21 February 2019, representatives of Europol and the Financial Crimes Enforcement Network (FinCEN) of the United States Department of the Treasury met to discuss possibilities for further cooperation, especially with regard to the exchange of financial information. The agencies agreed on the deployment of a FinCEN Liaison Officer to Europol to support and coordinate the cooperation between FinCEN, Europol, and EU Member States.

FinCEN carries out its mission by receiving and maintaining financial transactions data, which are analysed and disseminated for law enforcement purposes. It also regulates banks and other financial institutions as far as the combating (detection, reporting and prevention) of money laundering and the countering of terrorism financing are concerned. (CR)

EMSC Activity Report 2018 Published

On 25 March 2019, Europol's European Migrant Smuggling Centre (EMSC) published its activity report for the year 2018.

The EMSC was set up in February 2016 to support Member States' investigations and to increase cooperation and coordination among law enforcement agencies.

According to the report, with regard to migrant smuggling in 2018, the EMSC handled 3657 new cases and 18,234 messages received by Europol's Secure Information Exchange Network Application (SIENA). It also took part

in 39 Action Days against migrant smuggling. Even more new cases were received with regard to trafficking in human beings (1601 cases).

According to the migrant smuggling intelligence picture, the overall migration flow towards Europe decreased in 2018. At the same time, facilitated secondary movements increased. Common *modi operandi* for secondary movements observed in 2018 were – often life threatening – concealment methods, intra-Schengen flights by means of fraudulent documents, and misuse of asylum procedures. In the future, the report sees continued migratory pressure from African countries. New anonymising technologies are increasingly impeding the tracing or monitoring of criminal targets by law enforcement agencies.

Recent trends with regard to trafficking in human beings see persons being trafficked not only for the purpose of sexual exploitation but also for the purpose of labour exploitation, forced begging (including disabled victims), forced sham marriages between EU and third-country nationals, and, to a lesser extent, social benefit fraud. With regard to labour exploitation, the report expresses hope that the creation of the European Labour Agency will contribute to an improved response to these developments.

Lastly, the report sets out the EMSC's response to these crimes in the form of coordinated, EU-wide investigations. The approach focuses on high-value targets (HVT), namely those individuals that constitute the highest risk of serious and organised crime in the EU. In addition, the EMSC supports regional, operational platforms. Ultimately, an Information Clearing House (ICH) has been established to enhance the intelligence picture on organised migrant smuggling from source and transit countries.

Looking at the future, the EMSC will continue focusing on the identification of HVTs. Furthermore, a Joint Liaison Task Force on migrant smuggling (JLTF-MS) will be established at Europol. (CR)

Results of Action Week Against Human Trafficking

From 8–14 April 2019, Europol – together with 23 EU Member States, Iceland, Norway, and Switzerland – conducted an action week against trafficking in human beings for the purpose of labour exploitation. The action resulted in 46 arrests and the identification of 323 potential victims. During the operation, more than 50,000 persons and over 17,000 vehicles were checked. Visits were made to 5000 business premises and other locations. (CR)

Joint Cybercrime Action Taskforce Enlarged

Sweden and Poland have joined Europol's Joint Cybercrime Action Taskforce (J-CAT). J-CAT operates within Europol's European Cybercrime Centre (EC3) and aims to enhance collaboration between law enforcement authorities in tackling major cybercrime threats and facilitating cross-border investigations. The 24/7 taskforce primarily deals with cyber-dependent crimes, cross-crimal facilitators, transnational payment fraud, and child sexual exploitation. It was launched in September 2014 and today comprises cyber liaison officers from 15 countries (nine EU Member States and six non-EU countries) and 17 law enforcement agencies.

For 2019, J-CAT is planning four webinars in cooperation with CEPOL to raise awareness among law enforcement agencies about the taskforce and how to cooperate with it. (CR)

Operation MISMED 2

At the beginning of March 2019, Europol reported that operation MISMED 2 resulted in the seizure of illegally trafficked medicines worth more than €165 million, 435 arrests, and the disruption of 24 organised crime groups. The international operation (carried out between April and October 2018) was led by the French Gendarmerie Nationale and the Finnish customs service. Europol actively supported and coordinated the operation in which law enforcement, customs and health regulatory authorities from 16 countries participated. Seized products included not only opioid medicines, but also performance and image enhancing drugs and pharmaceutical products used for the treatment of major illnesses. (CR)

Frontex

Patrol Cars Started Operating

At the end of May 2019, for the first time in its history, Frontex started to operate its own patrol cars in various field deployments at Europe's borders.

The patrol cars are a first step towards Frontex operating its own equipment rather than relying on equipment from the EU Member States. This relieves the pressure on Member States participating in the agency's activities and enables Frontex to react more quickly to any developments at the EU's external borders. Other Frontex equipment planned for the future include own vans, vessels, planes, and remotely piloted aircraft. (CR)

First Operation Outside the EU

On 21 May 2019, Frontex launched its first full-fledged joint operation outside the European Union. This first operation in Albania aimed at supporting Albanian border guards with border control and at combating cross-border crime.

For the operation, 50 officers from 12 EU Member States, 16 patrol cars, and one thermo-vision van were deployed to Albania's border with Greece.

This new cooperation procedure was made possible by a status agreement on border cooperation between the EU and Albania on actions carried out by the European Border and Coast Guard Agency in the Republic of Albania. It came into force on 1 May 2019. The agreement covers all necessary aspects for carrying out actions (joint operations, rapid border interventions, and return operations) on the part of the Agency in the territory

of Albania. Executive powers are given to team members, i.e., Agency staff, border guards, and other relevant staff from participating Member States. An operational plan must be established detailing the organisational and procedural aspects for each operation. (CR)

Liaison Officer for Portugal and Spain Deployed

Within its strategy to deploy liaison officers to enhance the cooperation between Frontex and national authorities responsible for border management, returns and coast guard functions, Frontex introduced its liaison officer for Portugal and Spain at the beginning of March 2019. (CR)

Annual Report of the Consultative Forum Published

On 1 March 2019, the Frontex Consultative Forum on Fundamental Rights published its annual report for the year 2018. The report still sees inadequat staffing of the Agency's Fundamental Rights Office and raises concerns with respect to the independence of this office. The report also regrets that the revision of the 2011 Fundamental Rights Strategy was not a priority of 2018.

With regard to the Forum's activities, the report sets out its work to enhance child protection and safeguarding in Frontex operations, and to address gender considerations, for example by collecting sex- and age-disaggregated data. In addition, the Forum had issued several recommendations in 2018, i.e. on statelessness in Frontex activities, on the Agency's serious incident reporting mechanism for alleged breaches of fundamental rights, and the Agency's complaints mechanism. The Forum also provided support with regard to the Agency's training products and courses.

Looking at 2019, the report already underlines the changes that may arise due to the end of the term of office of the current Forum by mid-2019. Furthermore, it outlines the importance of the Forum's participation in the discussions on the European Commission's proposal to revise the European Border and Coast Guard Regulation. (CR)

Risk Analysis for 2019

On 20 February 2019, Frontex published its Risk Analysis for the year 2019.

According to the report, illegal border-crossings in 2018 amounted to 150,114 – 27% less than in 2017. The report sees the primary reason for this decrease in the dramatic fall in the number of migrants on the Central Mediterranean route. As a consequence, the spotlight moved onto the Western Mediterranean route, which had become the most frequently used route into Europe in 2018. The implementation of a relocation and return programme in Turkey for irregular Syrian migrants marked the most significant development of the Eastern Mediterranean route in 2018. It was also observed that the visa-free entry to the Russian Federation for the FIFA World Cup for those in possession of match tickets in 2018 created a temporary opportunity to reach the EU's external borders.

Looking at migrants' nationalities, the report finds Syrian, Moroccan, Afghan, and Iraqi migrants to be the top four nationalities in 2018.

Secondary movements continued on a large scale during 2018. Accordingly, the report finds a 13% increase in the inland detection of people smugglers as well as a significant increase in document fraud, which reached its highest level since 2013.

With 148 121 effective returns of migrants who were not granted asylum or subsidiary protection, the number of effective returns in 2018 once again fell short of the 286 875 decisions issued by Member States to return migrants.

Ultimately, the report underlines the increasing workload for border guards in Member States who were faced with another increase in entry and exit checks due to yet another rise in passenger flows [in 2018] and the 2017 expansion of systematic checks on those passengers enjoying the right of free movement under EU law. (CR)

Illegal Border Crossings in 2018

In 2018, the number of illegal border-crossings at Europe's external borders – at an estimated 150,000 – was at its lowest in five years. This drop was caused mainly by the Central Mediterranean route to Italy seeing the lowest number of irregular entries since 2012. However, the number of migrants taking the Western and Eastern Mediterranean routes increased in 2018, with the Western Mediterranean route now being the most active migratory route into Europe. (CR)

Agency for Fundamental Rights (FRA)

Fundamental Rights in the "Hotspots"

In 2016, FRA had published an Opinion on fundamental rights in the "hotspots" set up in Greece and Italy formulating "21 individual opinions to address the fundamental rights shortcomings identified in the implementation of the hotspot approach in Greece and Italy".

In March 2019, FRA published an update of the 2016 Opinion. Out of the 21 issues outlined in 2016, only three were properly addressed. For eight opinions, the update sees developments, however, without yet resulting in significant improvements on the ground. No significant progress was made for 10 out of the 21 issues outlined in 2016.

Issues properly addressed were the excessive use of force to take fingerprints, training for escorts deployed for readmissions, and the independent monitoring of return and readmission operations.

By contrast, no significant improvements at all have been achieved with regard to the following issues:

- Systemic delays in registering asylum applications of certain nationalities in the Greek hotspots;
- Delays with regard to the asylum procedure of unaccompanied children;

- Legal support for asylum applicants in the Greek hotspots;
- Material reception conditions;
- Systematic vetting procedures to ensure that individuals with a child abuse past do not engage with children in the hotspots;
- Lack of information on procedures and rights;
- Risk of gender-based violence due to inappropriate camp design and management;
- Risk of abuse and violence for children;
- Community engagement and outreach through regular meetings with asylum seekers and migrants hosted in the hotspots;
- Placement in pre-removal detention.

Therefore, the report strongly asks for the support of the EU and other EU Member States to take the load off these hotspots. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

Commission Presents New Anti-Fraud Strategy

spot light

More consistency, better coordination, and more data-driven anti-fraud measures – these are the main elements of the Commission's new Anti-Fraud Strategy (CAFS) that was tabled on 29 April 2019 in the form of a Communication (COM(2019) 196 final). The CAFS is an internal policy document that aims at enhancing action to protect the EU budget. It is binding for the Commission services and executive agencies in their fight against fraud and corruption affecting the EU's financial interests.

In essence, the new CAFS updates the Anti-Fraud Strategy of 2011 (2011 CAFS). The 2019 CAFS takes into account the 2011 CAFS review and also makes necessary adaptations to meet the challenges of an evolving and changing fraud landscape, e.g., new funding schemes and fraud trends, development of IT tools, etc.

Adaptations were also necessary in view of preparations for the new multi-annual financial framework (MFF) and two key legal developments in the EU's fight against fraud and financial irregularities in 2017: the adoption of the Directive on the fight against fraud to the Union's financial interests by means of criminal law (see eucrim 2/2017, 63–64) and the Regulation establishing the European Public Prosecutor's Office (see eucrim 3/2017, 102–104).

The Communication briefly takes stock of implementation and evaluation of the 2011 CAFS. Details of this evaluation, which also involved the executing authorities, are contained in an accompanying staff working document – the "Fraud Risk Assessment." The 2019 CAFS takes up central weaknesses identified by the fraud risk assessment, i.e.:

- Gaps in IT-supported collection and strategic analysis of fraud-related data;
- Lack of relevant and reliable indicators to successfully fight against fraud;
- Potential for more effective central coordination and oversight.

Some of these shortcomings were also addressed in a special report by the European Court of Auditors of 10 January 2019. Key recommendations in this report also taken up in the 2019 CAFS.

While the overall objectives and guiding principles of the 2011 CAFS remain fully relevant, the 2019 CAFS sets out two priority objectives:

- Data collection and analysis, with the aim of better understanding fraud patterns, fraudsters' profiles, and systemic vulnerabilities relating to fraud affecting the EU budget;
- Coordination, cooperation, and processes with the aim of optimising coordination, cooperation, and workflows in the fight against fraud, especially among Commission services and executive agencies.

Further objectives deriving from the guiding principles and the fraud risk assessment are:

- Integrity and compliance;
- Know-how and equipment;
- Transparency;
- Legal framework;
- Fighting revenue fraud.

All seven objectives are spelled out more clearly in an Annex to the Commission Communication on the new Anti-Fraud Strategy. An Action Plan further implements the strategy by detailing individual actions by which to achieve the objectives in the anti-fraud cycle, i.e. prevention and detection, investigations, corrective measures and sanctions, and reporting. This Action Plan will run until the next CAFS update, which is scheduled for the mid-term review in the upcoming MFF.

By placing importance on reinforcing the Commission's corporate oversight of fraud issues, OLAF will play a much stronger advisory and supervisory role in the future. OLAF is to conduct mandatory reviews of the anti-fraud strategies of all Commission Directorates and monitor their implementation. Stronger liaisons with all departments, especially with the Heads of the Commission's central services (Secretariat-General, Legal Service, DG Human Resources, and DG Budget), is also planned. In addition, the Commission will strengthen its follow-up of OLAF's recommendations in order to ensure better implementation.

Ultimately, OLAF is designated as the EU's lead service in the conception and development of European anti-fraud policy. Its role in corporate management will also become stronger. In this way, the 2019 CAFS complements the so-called "Governance Package" that was presented by the Commission in November 2018. (TW)

ECA: Action is Needed in the EU's Fight Against Fraud

In a special report of 10 January 2019, the European Court of Auditors (ECA) details weaknesses of the Commission's fight against fraud in EU spending.

OLAF's administrative investigations have resulted in recovery of less than a third of the unduly paid funds, the report states. Furthermore, only in about 45% of cases, OLAF investigations result in the criminal prosecution of suspected fraudsters.

The ECA further reprimands the Commission for not having comprehensive and comparable data on the scale, nature and causes of fraud. The Commission has so far also not carried out any assessment of undetected fraud. There is no detailed analysis to identify what causes some recipients of EU money to behave fraudulently. This lack of information reduces the practical value of the Commission's strategic plans, which partially need to be updated.

Incoherencies further exist in the internal governance structures of the Commission to detect and report fraud. Furthermore, the Commission does not fully verify the reliability of fraud information from the Member States.

In sum, *Juhan Parts*, the responsible rapporteur at the ECA, said that anti-fraud activities to date are still insufficient.

The report recommends the Commission doing the following:

- Putting in place a robust fraud reporting and measurement system, providing information on the scale, nature and root causes of fraud;
- Clearly referring to fraud risk management and prevention in one Commissioner's portfolio and adopting a renewed anti-fraud strategy based on a comprehensive risk analysis;
- Intensifying its fraud prevention activities and tools;
- Reconsidering OLAF's role and responsibilities in light of the establishment of the European Public Prosecutor's Office (EPPO) and giving OLAF a strategic and oversight role in EU anti-fraud action.

As regards the EPPO, the ECA considers its establishment a step into the right direction, but also warns of several risks. These include that detection and investigation is heavily dependent on national authorities, but the scheme did not put in place any mechanism enabling the EPPO to urge Member States to allocate the necessary resources to the new body.

Commissioner for Budget, *Guenther H. Oettinger,* rejected the auditors' allegations according to a news report from euractiv. He underlined that the Commission has "zero tolerance for fraud and corruption with EU funds." Furthermore, "there is nothing new in the anti-fraud policy recommendations that ECA tabled". "Most areas of improvement have long been identified and tackled already, or we are about to," Oettinger said.

As regards the ECA's critics over the EPPO, Oettinger pointed out that the new European Public Prosecutor's Office will be up and running by 2020, and that it will not need to rely upon traditional instruments of EU law for cooperation among judicial authorities of different member states. (TW)

EP Generally Supports Link Between Non-Respect of Rule of Law and Loss of EU Money

On 19 January 2019, the European Parliament adopted its position to the regulation on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States. In essence, the EP backs the idea of the Commission in its proposal of 2 May 2018 (see eucrim 1/2018, 12) that the EU may take appropriate measures in connection with EU funding against a Member States where generalised deficiencies as regards the rule of law persist. The measures may include suspending, reducing and restricting access to EU funding in a manner proportionate to the nature, gravity and scope of the deficiencies.

The EP, however, makes a number of proposals for amendments. These include the following:

- The notion of "generalised deficiency" as to the rule of law is defined more precisely (new Art. 2a). It includes endangering the independence of judiciary, failing to prevent, correct and sanction arbitrary or unlawful decisions by public authorities, limiting the availability and effectiveness of legal remedies, and measures that weaken the protection of the confidential communication between lawyer and client are listed as a criteria for possible generalised deficiencies.
- The risks for the financial interests of the EU are linked to the Copenhagen criteria – the essential conditions which each candidate country must fulfil before it can become a EU Member. These criteria include: the stability of institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities, a functioning market economy and the capacity to cope with competition and market forces, and the ability to take on the obligations of Union membership.
- The assessment of generalised deficiencies is clarified. To that end, the EP proposes that the Commission takes into account all relevant information, including information coming from the Parliament and from bodies such as the Venice Commission of the Council of Europe. The Commission must also take into account the criteria used in the context of accession negotiations.
- The Commission should be assisted in its assessment by a panel of independent experts for which also representatives of relevant organisations and networks can be invited as observers (new Art. 3a).
- Final beneficiaries should be better protected. Hence, the EP suggests that the Commission should take all appropriate measures to assist final beneficiaries in enforcing their claims when legal obligations are not respected.
- The EP must have a strengthened position in the procedure of appropriate measures in which the EP has – as the Council – a right to reject.

Other amendments relate to the improvement of the certainty of the procedure by including indicative deadlines for the Commission to react to information received from Member States.

The Council has not adopted a general approach on the proposal yet. (TW)

EDPS Opinion Combating VAT Fraud Related to E-Commerce

On 14 March 2019, the European Data Protection Supervisor (EDPS) issued an opinion on a legislative initiative that aims at curbing VAT fraud in the area of e-commerce. The initiative was tabled by the Commission in December 2018 and consists of two proposals, one for a directive amending Directive 2006/112/EC (COM(2018) 812 final) and another for a regulation amending Regulation (EU) No 904/2010 (COM(2018) 813 final). The proposals would create the following obligations for Member States:

- Ensuring that payment service providers keep records on cross-border payment transactions, so that tax authorities are able to detect VAT fraud;
- Enabling competent national authorities to collect, exchange, and analyse information on payment transactions;
- Establishing a central electronic information system (CESOP) where information stored at the national level is transmitted by Member States and would then be accessible by Eurofisc liaison officials. Eurofisc would analyse the information contained therein with the purpose of investigating tax fraud.

The EDPS makes specific recommendations on various parts of the Commission proposal. The recommendations aim at reducing the impact of the envisaged legislation on fundamental rights, thus ensuring compliance with the EU's data protection legal framework.

The EDPS welcomes the Commission's approach towards limiting the processing of data to the purpose of fighting tax fraud and also limiting the collection and use of personal data to the online business (payees) and not extending them to the consumers (payers). This approach should not be watered down during negotiations with the Council. The EDPS recommends, however, that specification of the purpose should not only be mentioned in the recitals, but also be inserted into the operative parts of legal acts.

Since a new central database is being created, the opinion recommends that the Commission follow the EDPS "Guidelines on the protection of personal data in IT governance and management of EU institutions" if the system is implemented and technical details have to be specified.

Ultimately, the EDPS opinion offers guidance on how to define the restriction on the data subject's rights in the proposed legislative acts. (TW)

Money Laundering

Directive on Better Law Enforcement Access to Financial Information on Way

The Council and European Parliament went ahead with the Commission's proposal for a directive laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA (COM(2018) 213, eucrim 1/2018, 13–14).

On 12 February 2019, the Romanian Council Presidency and the European Parliament reached an informal agreement on the directive. It will complement existing EU anti-money laundering rules by giving law enforcement authorities and asset recovery authorities direct, immediate, and timely access to national, centralised bank account registries and data retrieval systems. It will also improve cooperation between the national authorities, Europol, and the Financial Intelligence Units (FIUs).

On 17 April 2019, the plenary of the European Parliament adopted a legislative resolution on the directive at first reading. Amendments to the original Commission proposal include the following:

- Purpose of the Directive;
- Access by competent authorities to bank account information;
- Monitoring of access and searches;
- Requests for information to an FIU by competent authorities;
- Exchange of information between FIUs of different Member States;
- Exchange of information between Europol and FIUs;
- Processing of sensitive personal data.

It is now up to the Council to formally adopt the text of the new legislation. Once the directive enters into force, Member States will have 24 months to implement it into their national legislation. (TW)

Strengthening European Supervision on Anti-Money Laundering – EP and Council Agree

In March 2019, the European Parliament and the Council reached a provisional agreement on the reform of European rules that aim to strengthen the mandates, governance, and financing of the European Supervisory Authorities (ESAs). The reform will give the ESAs greater responsibility for ensuring the convergence of financial market supervision.

The so-called European System of Financial Supervision review package (the ESFS package) was complemented by an anti-money laundering/anti-terrorist financing (AML/CFT) component in September 2018 by the Commission (see eucrim 2/2018, 94). This component mainly aims to strengthen the role of the European Banking Authority (EBA) in preventing and mitigating risks of money laundering.

On 16 April 2019, the European Parliament adopted a legislative resolution on the package at first reading. As regards the AML/CFT section, the text reinforces the EBA's mandate and powers, e.g., by:

- Strengthening the provision of information to the EBA by competent national authorities;
- Developing common regulatory and supervisory standards with the aim of improving the prevention of and fight against money laundering and terrorist financing in the financial sector;

- Conducting peer reviews of competent authorities and risk assessment exercises;
- Assessing the strategies, capacities, and resources of the competent authorities dealing with emerging risks related to money laundering and terrorist financing;
- Giving the EBA a leading role in the coordination and cooperation between EU authorities and national authorities, including those in third countries.

It is now up to the Council to formally adopt the new legislation. (TW)

Council Opposes Commission's AML Blacklisting of Third Countries

At the meeting of 7 March 2019, the JHA Council unanimously rejected a list of 23 "high-risk third countries" in the area of money laundering and terrorist financing. The list was put forward by the Commission on 13 February 2019.

The list aims to protect the EU financial system by better preventing money laundering and terrorist financing risks. As a result of the listing, banks and other entities covered by EU anti-money laundering rules will be required to apply increased checks (due diligence) on financial operations involving customers and financial institutions from these high-risk third countries to better identify any suspicious money flows. The list was adopted on the basis of the fifth anti-money laundering directive that came into force in July 2018 (see eucrim 2/2018, 93). It is the result of an autonomous, in-depth assessment of the Commission.

The Council justified its rejection by stating that it "cannot support the current proposal that was not established in a transparent and resilient process that actively incentivises affected countries to take decisive action while also respecting their right to be heard."

The Commission must now draft a new list of high-risk third countries that takes into account the Member States' concerns. Although the Commission has the power to draw up the list by delegated act, the act must be approved by the Council and the European Parliament.

The list is a continuous bone of contention. Whereas MEPs backed the Commission's position, Member States' governments fear political pressure of important trade partner, such as Saudi Arabia or the U.S. (with four U.S. territories on the Commission's list). (TW)

New Infringements Proceedings for Incorrect Transposition of 4th AML Directive

In January 2019, the Commission has launched or went ahead with further infringement proceedings against EU Member States for not having correctly transposed the fourth Anti-Money-Laundering Directive. The infringement proceedings are in different stages. They concern Germany, Belgium, Finland, France, Lithuania, Portugal, Bulgaria, Cyprus, Poland and Slovakia. Infringement proceedings against other states are ongoing (see eucrim 3/2018, 152 and 2/2018, 93). (TW)

Non-Cash Means of Payment

New Directive Criminalises Fraud and Counterfeiting of Non-Cash Means of Payment

spot light

The European Parliament and the Council established new rules on combating fraud and the counterfeiting of non-cash means of payment. Directive 2019/713 was published in Official Journal L 123/18 of 10 May 2019. The Directive goes back to a Commission proposal of September 2017 (see eucrim 3/2017, 109 and eucrim 1/2018, 17). It replaces Council Framework Decision 2001/413/JHA and therefore "lisbonizes" another area of substantive criminal law.

The Directive above all harmonizes the criminal conduct of natural or legal persons in relation to non-cash means of payment. The reform of the Framework Decision was considered particularly necessary in order to update the EU response to new technologies involving payment instruments that are beneficial to business and consumers, on the one hand, but also increasingly benefit criminals, on the other. As a result, the new rules must also be seen in the context of the EU's efforts to provide better cybersecurity.

Directive 2019/713 includes common definitions in the areas of fraud and the counterfeiting of non-cash means of payment. Criminal liability has now also been extended to virtual currencies (insofar as they can be commonly used to make payments) and digital wallets.

The Directive defines the constituent elements of criminal conducts, which have been categorized as follows:

- Fraudulent use of non-cash payment instruments;
- Offences related to the fraudulent use of corporal non-cash payment instruments;
- Offences related to fraudulent use of non-corporal non-cash payment instruments;
- Fraud related to information systems;
- Tools used to commit offences.

The Directive clarifies that incitement, aiding and abetting, and attempt of any of the above-mentioned offences must also be made punishable as a criminal offence.

As another main element, the Directive lays down minimum rules for sanctions and penalties for natural and legal persons. The Directive follows the common EU approach of defining minimum/maximum terms of penalties. Depending on the offence, maximum terms of imprisonment for natural persons range from at least one to three years. More severe penalties apply if a crime is committed within the framework of a criminal organisation (as defined in Framework Decision 2008/841/JHA).

The Directive also includes rules on the following issues:

- Jurisdiction and conflicts of jurisdiction;
- Investigative tools to effectively investigate fraud and the counterfeiting of non-cash means of payments;

- Exchange of information by national points of contact that are available 24/7;
- Establishment of channels that facilitate reporting of the offences described in the Directive;
- Encouragement for financial institutions and other legal persons to report suspected fraud or counterfeiting to law enforcement authorities.

The Directive also strengthens the assistance to and support of victims – provisions that were mainly shaped by the European Parliament during the negotiations. It adapts the rights of victims under Directive 2012/29 to the special needs of victims of fraud in conjunction with non-cash means of payment. In this context, the Directive, *inter alia*, obliges Member States to ensure that natural and legal persons can obtain specific information and advice on how to protect themselves against the negative consequences of the offences, e.g., reputational damage. A list of dedicated institutions that deal with different aspects of identity-related crime and victim support is also provided. Furthermore, Member States are encouraged to set up single, national online information tools to facilitate access to assistance and support for victims whose personal data were misused.

Member States must implement the provisions of the Directive by 31 May 2021. The Commission has been called upon to submit an implementation report by 31 May 2023 and carry out an evaluation on the impact of the Directive by 31 May 2026. (TW)

Organised Crime

EMPACT 2018 Results and 2019 Operational Action Plan on Financial Crime

In December 2018, the European multidisciplinary platform against criminal threats (EMPACT) published its results for the year 2018, stating that 1026 investigations had been initiated with over €1.4 million seized in cash during the EMPACT Joint Action days. Furthermore, 1137 suspects were arrested and 337 victims of human trafficking identified. EMPACT's priority areas of crime in 2018 included cybercrime, drug trafficking, the facilitation of illegal immigration, organised property crime, trafficking in human beings, excise and MTIC fraud, illicit firearms trafficking, environmental crime, criminal finances, and money laundering as well as document fraud.

Furthermore, in January 2019, the 2019 Operational Action Plan for the EMPACT priority "Criminal Finances, Money Laundering and Asset Recovery" was kicked off with a meeting at Europol. The action plan outlines 19 actions targeting criminal finances, money laundering, and asset recovery. The actions will be carried out throughout Europe. The action plan intends to coordinate law enforcement work in this criminal area. The meeting was attended by financial crime investigators from 25 EU Member States as well as specialists from Europol, CEPOL, and the European Commission.

EMPACT is an acronym for the European Multidisciplinary Cooperation Platform Against Criminal Threats. It offers an *ad hoc* management environment to develop activities in order to achieve pre-set goals. EMPACT enlists the support of several EU Member States, EU institutions, and agencies as well as third countries, international organisations, and other public and private partners aiming to address the main threats of organised and serious international crime. The multiannual EU's Policy Cycle prioritises the threats. In March 2017, the policy cycle was renewed for the 2018–2021 period. (CR)

Cybercrime

ECA Dissatisfied with EU's Cybersecurity Performance

Multiple challenges exist to strengthen EU's cybersecurity and its digital autonomy, and the EU needs to do more. This is the main outcome of a briefing paper by the European Court of Auditors (ECA) that was published on 19 March 2019.

The briefing paper provides an overview of the EU's cybersecurity policy landscape and identifies major challenges to effective policy delivery. It covers network and information security, cybercrime, cyber defence, and disinformation. The majority of research was carried out between April and September 2018; developments up to December 2018 were taken into account.

The challenges are grouped into four clusters:

- The policy framework;
- Funding and spending;
- Building cyber-resilience;
- Responding effectively to cyber incidents.

Each chapter ends with reflection points that are addressed to policymakers, legislators, and practitioners.

The authors of the briefing paper conclude that the EU's ambition to become the world's safest digital environment is a monumental task. In order to achieve accountability, the EU needs to shift towards a performance culture with embedded evaluation practices.

Gaps remain in existing legislation that is not being consistently transposed by the EU Member States. As a result, legislation cannot reach its full potential.

Another significant challenge is to overcome fragmented spending in the cybersecurity research field. There is no clear picture of funding and spending. Investments must be aligned with strategic goals. The paper also addresses constraints in the adequate resourcing of the EU's relevant cybersecurity agencies which entails difficulties in attracting and retaining talents.

As regards building cyber-resilience, the ECA notes that there is a global weakness in cybersecurity governance, which impairs the global community's ability to respond to and prevent cyber-attacks. Governance issues also impede

the EU's aim to take a coherent approach. The ECA recommends improving skills and awareness across all sectors in order to overcome the growing global skills shortfall. This must be flanked by better information exchange and coordination between the public and private sectors.

For an effective response to cyber-attacks, key challenges for the EU remain rapid detection and response as well as protection of critical infrastructure and societal functions. In the latter context, further challenges are posed by potential interference in electoral processes and disinformation campaigns, especially in view of European Parliament elections. (TW)

ENISA Report on Cyberthreat Landscape

The cyberthreat landscape changed significantly in 2018; the risk of becoming the victim of a cyberattack remains high. This is one of the main conclusions of the 2018 Threat Landscape Report by the European Union Agency for Network and Information Security (ENISA). The report (in short "ETL 2018") was released on 28 January 2019.

The ETL 2018 gives an overview of cyberthreat intelligence and provides in-depth analyses of the top 15 cyberthreats, e.g,. malware, web-based attacks, phishing, and botnets. In addition, the report includes analyses on trends and motives in relation to threat agents and attack vectors.

In 2018, the motives and tactics of the most daunting threat agent, namely cyber-criminals and state-sponsored agents, continued to develop. Cyberjacking is new on the list of the top 15 threats. State-sponsored agents increasingly tend to apply low-profile social engineering attacks, thus shifting away from using complex malicious software and infrastructures.

On the positive side, the report states that defence against cyberattacks and cybercrime has progressed. In particular, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts. The combination of cyberthreat intelligence and traditional intelligence has also proven to be a successful approach that is to be pursued further. Increased training efforts resulted in better skills and capabilities which is an important factor in building up cyber-resilience.

The identified trends and the need for targeted actions led the ELT 2018 to make several conclusions in the areas of policy, business, and research/education:

- The EU must increase its personnel and technical capabilities in cyberthreat intelligence;
- Regulatory barriers to collecting cyberthreat intelligence should be removed;
- Businesses should make cyberthreat intelligence available to a greater number of stakeholders, especially those who lack technical knowledge;
- Businesses should counteract risks and threats along the entire supply chain;
- Accurate information on incidents and information from related disciplines is crucial for knowledge of cyberthreat intelligence; vendors and researchers must find ways to enlarge the scope of cyberthreat intelligence;
- Knowledge management should be standardised, e.g., by standard vocabularies, standard attack repositories, or automated information collection methods;
- Research should be carried out particularly in the areas of attack practices, malware, malicious infrastructures, and threat agent profiling.

ENISA's Executive Director *Udo Helmbrecht* said that the ETL 2018 "provides recommendations as to how the digital single market can prepare an adequate response to cyber threats, with certification and standardisation at the forefront." (TW)

Cyber-Telecom Crime Report 2019 Published

In April 2019, Europol's European Cybercrime Centre (EC3) and Trend Micro Research published a joint Cyber-Telecom Crime Report 2019. Trend Micro is a global provider of enterprise data security and cybersecurity solutions.

The report intends to help stakeholders in the industry navigate the telecom threat landscape. It offers an overview of how telecom fraud/crimes translate into monetary gains for criminals and explains key concepts of the telecom infrastructure.

At the heart of the report are threats concerning infrastructure attacks and network-based telecom frauds. The report also offers a number of case studies of relevant telecom fraud cases to demonstrate how these attacks play out in real-world situations. (CR)

Cryptocurrency Mixing Service Taken Down

On 22 May 2019, one of the world's leading cryptocurrency mixing services 'Bestmixer.io' was shut down in a joint action of the Dutch Fiscal Information and Investigation Service (FIOD) in cooperation with authorities in Luxembourg and at Europol.

A cryptocurrency mixing service offers to mix potentially identifiable cryptocurrency funds with other funds in order to obscure the trail back to the fund's original source.

Bestmixer.io was one of the three largest mixing services for cryptocurrencies, with an annual turnover of at least US-$200 million (approx. 27,000 bitcoins). It offered services for mixing the bitcoins, bitcoin cash, and litecoins. Customers remained anonymous.

Investigations undertaken so far reveal that many of the mixed cryptocurrencies on Bestmixer.io had a criminal origin or destination, probably to conceal and launder criminal flows of money. (CR)

Malware Group Dismantled

In mid-May 2019, GozNym, a cybercriminal network offering cybercrime as a service was able to be dismantled through an international operation between Bulgaria, Georgia, Germany,

Moldova, Ukraine, and the USA. Criminal services offered by GozNym included, for instance, bulletproof hosters, money mule networks, crypters, spammers, coders, organizers, and technical support.

By means of a complex system of recruited cybercriminals and spammers, the head of GozNym controlled more than 41,000 victim computers infected with GozNym malware. The malware captured the victims' online banking login credentials with the aim of fraudulently gaining unauthorised access to their online bank accounts. (CR)

Dark Web Marketplaces Taken Down

At the beginning of May 2019, two major dark web marketplaces, the "Wall Street Market" and the "Silkkitie" (known as the Valhalla Marketplace), were taken down in an international operation between Dutch, Finnish, French, German, and several US authorities together with the support of Europol and Eurojust.

Wall Street Market was the world's second largest dark web market, aiming at international trade in criminal goods, drug trade (including cocaine, heroin, cannabis, and amphetamines), stolen data, fake documents, and malicious software. The marketplace had over 1,150,000 customer accounts, 5400 registered sellers, and 63,000 sales on offer.

Silkkitie had been in operation since 2013, mainly offering narcotics and other illicit goods. (CR)

Racism and Xenophobia

EP Adopts Position on Proposed Regulation of Terrorist Content Online

The Commission proposal for a Regulation on preventing the dissemination of terrorist content online of September 2018 (see eucrim 2/2018, 97–98 and the article by *G. Robinson*, eucrim 4/2018, 234) underwent scrutiny by the Union legislators, i.e., the Council and the European Parliament. Both institutions proposed several amendments. The start of trilogue negotiations is expected after the new European Parliament becomes operational in autumn 2019 following the May 2019 elections.

The proposed EU legislation is addressed to hosting service providers operating in EU territory. They will be obliged to take down terrorist content or disable access to it within one hour of receiving a removal order from the authorities. If they fail to comply, they may be liable to a penalty of up to max. 4% of their global turnover for the previous year. In addition, they are to apply certain duties of care to prevent the dissemination of terrorist content on their Internet platforms and to take proactive measures.

The Council already agreed on its general approach at the beginning of December 2018 (see eucrim 4/2018, 199).

At first reading, the plenary of the European Parliament adopted a legislative resolution on 17 April 2019. It backs the position elaborated by *Daniel Dalton* (UK, European Conservatives and Reformists Group) as the main rapporteur in the LIBE committee. Essential amendments compared to the Commission proposal relate to purpose and scope of the Regulation, the definition of terrorist content, due diligence obligations and removal orders, proactive measures, transparency obligations, and sanctioning.

MEPs clarified that the new EU legislation does not entail a general monitoring obligation for online platforms and does not force them to use filters. MEPs also stressed that the new rules must safeguard free speech and press freedom. (TW)

EDPS Comments on Terrorist Content Online Regulation

On 12 February 2019, the European Data Supervisor (EDPS) tabled "formal comments" on the Commission proposal for a regulation on preventing the dissemination of terrorist content online (see eucrim 2/2018, 97–98 and the article by *G. Robinson*, eucrim 4/2018, 234).

The EDPS generally supports the proposal's objective to set up binding, harmonised rules for host service providers (HSPs), who offer services within the territory of the Union, in order to prevent the dissemination of terrorist content through their platforms and to ensure its swift removal. The EDPS, however, sees several possible improvements that could reduce conflicts over the fundamental rights to privacy and to the protection of personal data.

The EDPS calls on the legislator to clearly describe all actions to be taken by HSPs pursuant to the proposal and to ensure adequate oversight by clearly identified, competent public authorities. The EDPS feels that this precision would help address concerns about the "privatisation" of law enforcement and be in keeping with the principles of quality of law and economic certainty.

The legislator should hence be as specific as possible as regards the information in the removal order issued by law enforcement authorities.

Beyond these general remarks, the EDPS specifically recommends that the definitions "terrorist content," "dissemination of terrorist content," and "host service providers" should be made more consistent and be aligned with existing EU law, e.g., Directive 2017/541 on combating terrorism.

As regards the obligation for HSPs to carry out a takedown decision within one hour after receipt of a removal order from the competent authorities, the EDPS points out that this could be especially challenging for small- and medium-sized companies. It may deprive HSPs from carrying out a meaningful check on the removal order.

One focus of the EDPS' comments is on the obligation for HSPs to take proactive measures. EU rules must take into account the principles of necessity and proportionality. This can be achieved by introducing two obligations when HSPs put in place proactive measures, i.e., HSPs should do the following:

- Perform and make public a risk assessment on the level of exposure to terrorism content (also based on the number of removal orders and referrals received);
- Draw up a remedial action plan to tackle terrorist content proportionate to the level of risk identified.

The EDPS eyes the elements of the proposal that include use of automated tools in the context of proactive measures. He stresses that EU legislation cannot lead to "automated individual decision-making" (prohibited by the GDPR). Therefore, removals based on automated tools must always be subject to human oversight and verification where appropriate. Reporting obligations for HSPs also need to be introduced in order to ensure that automated tools do not produce discriminatory, untargeted, unspecific, or unjustified results.

Furthermore, the EDPS recommends reconsidering the rules on mandatory preservation of terrorist content and "related data" since they are not compatible with the CJEU's case law on data retention.

Ultimately, the EDPS takes issue with the envisaged complaint mechanism within the HSPs. Though welcome, EU legislation should introduce deadlines for HSPs by which a decision on a complaint must be taken. (TW)

EESC Opinion on Terrorist Content Online Regulation

In an opinion published in the Official Journal C 110/67 of 22 March 2019, the European Economic and Social Committee (EESC) largely welcomed the initiative for a regulation on preventing the dissemination of terrorist content online (see eucrim 2/2018, 97–98 and the article by *G. Robinson*, eucrim 4/2018, 234). The new rules must uphold the right to freedom at stake, which essentially means that access to effective legal protection and to fair and prompt proceedings must be ensured.

The EESC, *inter alia*, recommends the following:

- Clear definition of vague legal concepts, such as "terrorist information," "terrorist acts," "terrorist groups," and "glorifying terrorism;"
- Although technical means of prevention (e.g., algorithms) are useful, accurate assessment of content by means of human, not technical (e.g., algorithmic), interventions for prevention purposes;
- No censorship or forced self-censorship on the Internet;
- Legislation must be aligned to the needs of small- and medium-sized companies that regularly do not have the technical, human, or financial capacities to act effectively against terrorist content;
- Users must be clearly reminded of the existing national rules on the production of terrorist content. The right to appeal against an administrative decision must be guaranteed, along with a clear explanation of this right and online tools for its exercise.

Since the proposed Regulation is based on the EU's competence to approximate rules for the functioning of the internal market (Art. 114(1) TFEU), the EESC must be consulted. However, its opinion is not binding for the EU co-legislators, namely the European Parliament and the Council. (TW)

DAV: Commission's Plans to Remove Terrorist Content Online May Infringe Freedom of Expression

In January 2019, the German Bar Association (Deutscher Anwaltverein – DAV) tabled a critical statement on the Commission's proposal for a regulation on preventing the dissemination of terrorist content online (for the proposal, see eucrim 2/2018, 97–98 and G. Robinson, eucrim 4/2018, 234–240).

First, the DAV has considerable doubts as to whether the EU has sufficient competence to adopt such legal instrument. The Commission has particularly not proved that a regulation can be based on Art. 114 TFEU and is necessary to achieve the articles' objectives of functioning the internal market. Furthermore, the focus of the instrument is actually on the prevention of risks of terrorist content and law enforcement, so that the instrument cannot but be based on one of the provisions of Title V, i.e., the area of freedom, security and justice. Finally, the Commission had not sufficiently taken into account the CJEU case law which acknowledges that measures of public security and law enforcement cannot be based on internal market.

Second, the DAV notes that the definition of "terrorist content" remains vague and unclear. Due to the ambiguities, hosting service providers may feel compelled to remove information from the Internet "in case of doubt." This constitutes a serious threat to freedom of expression.

Finally, the DAV criticises the plans for the removal orders, referrals and proactive measures. The DAV sees here infringements of the companies' freedom to conduct business. The statement also clarifies that the instrument transfers tasks of the state to private entities without providing for the necessary flanking measures. (TW)

Commission: Code of Conduct with IT Companies to Tackle Hate Speech is Evolving Positively

On 4 February 2019, the Commission presented its fourth evaluation of the Code of Conduct on Countering Illegal Hate Speech Online. The Code of Conduct was launched on 21 May 2016 and aims that requests to remove racist and xenophobic Internet content are dealt quickly by the major IT companies (see also eucrim 2/2016, p. 76; for last years' evaluation, see eucrim 1/2018, p. 18). Currently, nine companies adhere to the Code, namely Facebook, YouTube, Twitter, Microsoft, Instagram, Google+, Dailymotion, Snapchat, and Webedia.

The evaluation report confirms that the Code of Conduct delivered continuous progress and the IT companies meanwhile provide a swift response to notified illegal hate speech online. About 89% of the notifications are as-

sessed within 24 hours. The IT companies fully meet the target of reviewing the majority of notifications within 24 hours. On average, IT companies are removing almost 72% of illegal hate speech incidents notified to them by the NGOs and public bodies participating in the evaluation. If it comes to serious cases of deemed illegal hate speech, such as calls for murder or holocaust denial, the average removal rate is even higher. Other major results of the evaluation include the following:

- There is no sign of over-removal;
- The actions on promoting positive narratives of tolerance and pluralism were positive;
- More efforts are needed on transparency and feedback to users.

The Code of Conduct is a self-regulatory instrument and not binding. It must be considered an additional tool of the EU's and Member States' efforts to tackle the proliferation of hatred online. (TW)

Procedural Criminal Law

Procedural Safeguards

CJEU: Rules on Exclusion of Unlawfully Obtained Evidence Precede Anti-Fraud Obligations

spot light

Do Art. 325 TFEU and the PIF Convention – read in the light of the principle of effective prosecution of VAT offences – restrict the applicability of national rules on the inadmissibility of evidence? This question was at the centre of the CJEU's judgment of 17 January 2018 in the case C-310/16 (criminal proceedings against *Peter Dzivev, Galina Angelova, Georgi Dimov, Milko Velkov*).

➤ *Facts of the Case and Legal Question*

The judgment concerned a request for a preliminary ruling from the *Spetsializiran nakazatelen sad* (Specialised Criminal Court, Bulgaria). The referring court had to decide whether the defendants could be convicted of VAT evasion. The court observed that interception of defendants' telecommunication were authorised by a court that had no longer jurisdiction after a reform of the Bulgarian Code of Criminal Procedure in 2012. The court added, however, the following:

- None of the authorisations were reasoned;
- The interceptions felt into a transitional phase before and after the reform of the Code of Criminal Procedure, and transitional rules were unclear that governed the transfer of the jurisdiction to the courts competent to authorise "special investigation methods" after the reform;
- In the case of Mr Dzivev, only the interceptions of telecommunications initiated on the basis of authorisations granted by the court which lacked jurisdiction clearly establish the commission of the tax offences he was accused for.

Against this background, the referring court wonders whether reliance on the illegally obtained evidence (here: wiretapping) would counteract the Member States obligations in particular from Art. 325 TFEU and Art. 2(1), 1(1) (b) of the Convention on the protection of the European Communities' financial interests ("PIF Convention") that, as established by previous CJEU case law, require the effective criminalisation of VAT fraud.

➤ *The CJEU's Decision and Reasoning*

At first, the CJEU reiterated the main aspects from previous case law regarding the obligations stemming from Art. 325 TFEU. Reference is particularly made to the decisions in *WebMindLicences* (C-419/14; cf. V. Covolo, eucrim 3/2016, 146); *M.A.S. and M.B.* (C-42/17, cf. eucrim 4/2017, 168); *Scialdone* (C-574/15, cf. eucrim 2/2018, 95); and *Kolev and Kostadinov* (C-612/15, cf. eucrim 2/2018, 99):

- The procedure for taking evidence and the use of evidence in VAT-related criminal proceedings is within the competence of the Member States;
- Member States must, however, counter fraud and other illegal activities affecting the EU's financial interests through effective, and deterrent measures;
- There is a direct link between the collection of VAT revenue (in compliance with the EU law) and the availability to the EU budget of the corresponding VAT resources;
- Criminal penalties may be essential to combat certain serious cases of VAT evasion in an effective and dissuasive manner as required by the PIF Convention;
- Infringements of EU law must be penalised under (procedural and substantive) conditions, which are analogous to those applicable to infringements of national law of a similar nature and importance; in any event, these conditions must make the penalty effective, proportionate and dissuasive;
- Rules of national criminal procedure must permit effective investigation and prosecution of offences linked to such conduct.

Although the Member States have procedural and institutional autonomy to counter infringements of harmonised VAT rules, this autonomy is, *inter alia*, limited by the principle of effectiveness. National courts may be obliged to disapply national provisions which, in connection with (criminal) proceedings concerning serious VAT infringements, prevent the application of effective and deterrent penalties.

The CJEU, however, stresses that these obligations have their limits, i.e. "the effective collection of the European Union's resources does not dispense national courts from the necessary observance of the fundamental rights guaranteed by the Charter and of the general principles of EU law, given that the criminal proceedings instigated for VAT offences amount to an implementation of EU law, within the meaning of Article 51(1) of the Charter. In criminal law, those rights and those principles must be respected not only during the

criminal proceedings, but also during the stage of the preliminary investigation, from the moment when the person concerned becomes an accused."

The authorities must act within the legal limits because they must observe the principles of legality and the rule of law. In addition, the interception of telecommunications amount to an interference with the right to a private life, and must therefore observe the requirements of Art. 7 CFR.

Transferring these yardsticks to the present case, the CJEU concludes that "it is common ground that the interception of telecommunications at issue in the main proceedings was authorised by a court which did not have the necessary jurisdiction. The interception of those telecommunications must therefore be regarded as not being in accordance with the law, within the meaning of Article 52(1) of the Charter."

As a result, EU law cannot require a national court to disapply the national rules on the exclusion of illegally obtained evidence, even if the evidence could "increase the effectiveness of criminal prosecutions enabling national authorities, in some cases, to penalise non-compliance with EU law".

The CJEU added that the following aspect pointed out by the referring court are irrelevant:

- The unlawful act committed was due to the imprecise nature of the provision transferring power to the competent court;
- Only the interception of telecommunications initiated on the basis of authorisations granted by a court lacking jurisdiction could prove the guilt of one of the four defendants in the main proceedings.

➤ *Put in Focus*

In sum, the CJEU follows the – much more detailed – opinion of AG *Bobek* of 25 July 2018.

The judgment summarises the cornerstones of the CJEU case law in relation to the protection of the financial interests. It was mainly developed in recent judgments (see above) that clarified the borders between procedural and institutional autonomy of the Member States to counter fraud affecting the EU's financial interests and common obligations stemming from EU law, including the principles of effectiveness, proportionality and equivalence. The judgment is a further "brick in the wall" as regards the question which procedural rules remain untouched by EU law. After the force of *res judicata* in *XC and Others* (C-234/17, cf. eucrim 3/2018, 142), the CJEU adds the rules on the exclusion of evidence to its list of important principles of national procedural law that precede the effectiveness of EU law. (TW)

CJEU: EU Law Does Not Govern the Procedure for Reviewing Pre-Trial Detention Decisions

Directive 2016/343 on the strengthening of certain aspects of the presumption of innocence does not govern the rules on how to examine evidence for confirming or maintaining pre-trial detention. The CJEU reiterated this position as already stated in its judgment of 19 September 2018 in case C-310/18 PPU (*Milev II*, see eucrim 3/2018, 155).

In the case at issue (C-8/19 PPU, *RH*), the referring Bulgarian Specialised Criminal Court had difficulties in formulating reasonable grounds for upholding pre-trial detention against RH (who was suspected of being part of a criminal gang organized in order to commit murders) on account of the Directive's aim that a person should not be presented as guilty. Furthermore, the referring court raised the question of compatibility of Bulgarian case law with EU law because the possibility to make preliminary ruling references to the CJEU is limited due to the obligation to adjudicate a criminal case within a reasonable time.

The CJEU first examined the latter question and stressed that national legislation is not acceptable if it results in the national court's obligation to adjudicate on the legality of a pre-trial detention decision without the opportunity to make a request for a preliminary ruling to the CJEU or to wait for its reply. In this context, the CJEU refers to the urgent procedure before the Court which constitutes an implementation of the right of all persons to have their case heard within a reasonable time. In addition, the CJEU stresses that judges cannot be exposed to disciplinary sanctions for exercising their choice to send a request for a preliminary ruling to the CJEU or not. This choice is an important element of judicial independence.

As to the material question, by referring to its judgment in *Milev II*, the CJEU clarifies that Directive 2016/343 in Articles 4 and 6 as well as Recital 16 widely exempts pre-trial detention from its scope. Therefore, secondary EU law does not include rules on how to review the legality of pre-trial detention, i.e., to which extent a national court is obliged to compare the elements of incriminating and exculpatory evidence presented to it and to provide reasoning via-à-vis the objections of the defence counsel. However, that decision may not present the person detained as being guilty. (TW)

AG: Italian Rules Restricting Negotiated Settlements in Line with EU Law

Procedural rules of national law that limit the accused person's possibility to request a negotiated penalty to the beginning of the trial are in conformity with EU law, according to the opinion of Advocate General (AG) *Bobek* in Case C-646/17 (criminal proceedings against *Gianluca Moro*). Neither the provisions of Directive 2012/13/EU on the right to information in criminal proceedings nor Art. 48(2) of the Charter alter this finding.

In the case at issue that was referred by the Tribunale di Brindisi, Italy, the defendant (Mr. Moro) had been charged with the criminal offence of handling proceeds of crime. After the start of the

trial, he was informed that the acts of which he was accused must be reclassified and that the charge could be modified to the criminal charge of theft. The defendant then applied for a negotiated penalty, known as "*patteggiamento.*" Under Italian law, however, such an application is only admissible before the trial proceedings have been opened if a mere legal reclassification of the acts occurs. At a later stage, the application is possible if the change is only of factual nature which was not the case here. The referring court was unsure whether this legal situation is in line with the provisions of Directive 2012/13 and Art. 48(2) of the Charter.

The AG first examined the general applicability of Directive 2012/13, especially since the Italian government put forth that the Directive is only applicable if there is a cross-border element in the main proceedings. The AG rejected this objection by arguing that the Directive is also applicable to cases that have a purely national dimension. Beside the wording, it is in particular the Directive's objective of the Directive that does not limit it to cross-border situations: the Directive pursues the harmonization of the Member States' criminal law systems in order to create a common playing field in which certain minimum standards are guaranteed.

Second, the AG agrees with the position of several Member States and the Commission that the legal question at issue, i.e., the consequences of the legal (re)classification of the accusation, is not governed by the provisions of Directive 2012/13. Challenging the ability to apply for a negotiated penalty at a given stage of the criminal procedure would be an overinclusion into the Directive. The AG especially focuses on Art. 6(4) of the Directive, which regulates the accused person's right to be informed of any changes in the accusation, "where this is necessary to safeguard the fairness of the proceedings." According to the AG, Art. 6(4) intends to enable the accused person to understand, respond to, and dispute the accusation (and the change thereto), but does not entail the obligation for the national courts to provide all information on any and every consequence of that change. The notion of the "fairness of the proceedings" does not alter this result because it correlates with the material scope of the rights enshrined in the Directive.

Ultimately, the AG examined the implications of Art. 48(2) of the Charter and concludes that it cannot be used to expand the scope and content of the procedural obligations defined in the respective EU secondary law. In other words: there is no obligation beyond what already exists in Directive 2012/13.

As a result, EU law does not preclude procedural rules such as the ones at issue, which allow the accused person to request a negotiated penalty after the beginning of the trial only if there is a change in the accusation that is of factual nature and not when the change is of a legal nature. (TW)

Data Protection

Collection of PNR Data Under Judicial Scrutiny in Germany

The debate on the retention of passenger name records (PNR) data has gained new momentum in Germany. On 14 May 2019, the "Gesellschaft für Freiheitsrechte" (GFF) informed the public that it brought actions before the administrative court of Wiesbaden and other local civil law courts in order to tackle the collection, use, and processing of PNR data by the German authorities. As from May 2018, airlines are obliged to transmit dozens of PNR to the centralised Passenger Information Unit, which belongs to the Federal Police Office (*Bundeskriminalamt – BKA*), if they operate third-country or intra-EU flights.

The BKA is entitled to check the data against police search databases (i.e., the German INPOL system or the Schengen Information System) and against patterns, in order to identify persons that allegedly committed certain serious crimes as defined in the German Act on the Processing of Air Passenger Data. The PNR can be stored for a period of five years. The Act implements EU Directive 2016/681 of 27 April 2016 "on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime" (see eucrim 2/2016, 78).

The actions of the GFF encourage the German courts to file references for preliminary rulings to the European Court of Justice. The judges in Luxembourg are to verify whether the EU PNR Directive complies with the EU's fundamental rights. The GFF argues that the retention of PNR data of anyone for a long period of time breaches the fundamental rights enshrined in Arts. 7 and 8 CFR. It is submitted that this position is also backed by the 2017 CJEU judgment that declared the agreement between the EU and Canada on the exchange of PNR data void (see eucrim 3/2017, 114–115).

The GFF closely cooperates with the Austrian organisation "epicenter.works," which lodged data protection complaints against PNR in Austria.

The complainants point out that there is no evidence that the retention of PNR has led to tangible results in detecting criminals or suspicious air movements. Data on first experiences with the PNR scheme in Germany underpin this finding. In a response of 17 April 2019 to questions from MPs representing the left-wing party "Die Linke," the German Federal Ministry of the Interior confirmed that, up to 31 March 2019, the automated "comparison processing system" had led to 94,098 hits – after an individual, manual assessment of the hits by law enforcement officers, however, follow-up measures (arrest, open or covert controls) were only undertaken in 277 cases. Critics therefore remark that almost all hits turned out to be waste data. (TW)

Report

"Freedom AND Security – Killing the zero sum process #kill0sum"

22–23 November 2018, The Hague

Europol published a conference report of an inspiring, not conventional data protection conference that took place in the Europol headquarters in autumn 2018.

Speakers and participants came from different sectors all over the world, including practicing officials and lawyers, data protection officers, academics, policy makers, members of civil society organisations, and staff from private enterprises. The event also convened members of EDEN, the Europol Data Protection Experts Network.

Daniel Drewer, Data Protection Officer of Europol, welcomed the guests by explaining the idea behind the conference. It posits that any notion of balancing "freedom versus security" wrongfully implies a unitary dial: if we turn up freedom, we get less security, and if we turn down freedom, we get more security. Freedom and security are viewed as a zero-sum trade-off. There is no doubt that there is a relation between freedom and security: A change to one will sometimes affect the other. But often it is also possible to increase security without decreasing freedom, and sometimes a decrease in our freedoms leads to no meaningful increase in security.

The EDEN conference aimed at developing a platform for an open discussion on the topic of data protection in a law enforcement context. Hence, many assumptions and prejudices were challenged.

The conference report summarises the main statements and results of the different panels that included:

- Keynote speech of the Assistant Supervisor at the EDPS;
- Impact of GDPR on law enforcement;
- Data as the new oil? Risks and opportunities for citizens and law enforcement;
- Data as the hostage – ransomware is still alive!
- The take-down of Hansa – at times the Darknet ain't that dark!
- The death of data retention at EU level – the mass surveillance scandal fallout and its detrimental consequences for law enforcement;
- Data protection by design for cooperation between law enforcement and intelligence services;
- From law enforcement fiction to future – will there be any privacy left in 2030, anyway?

The next EDEN conference will take place in Copenhagen. (TW)

Retention of Telecommunications Data Continue to Be on the Text Bench

After the Council launched a reflection process on the retention of telecommunications data, and after an exchange of views on the state of play and the way forward at the JHA Council meeting of 6–7 December 2018 (see eucrim 4/2018, 201), work continued on the technical and working levels. Under Europol's coordination, experts agreed on a number of aspects to be considered in a possible future, new EU data retention law. These aspects include a matrix of limited data categories, the length of the retention period, rules on erasure, data security, etc.

In April 2019, the Council Working Party DAPIX discussed Council conclusions that called on the Commission to start a series of consultations with relevant stakeholders and to prepare a "comprehensive study" on possible solutions for the retention of telecommunications data for law enforcement purposes. The study should also include concepts that meet the requirements of the CJEU's case law on the various interference levels of the data retention regime. In 2014, the CJEU had declared the 2006 EU data retention directive void (see eucrim 1/2014, 12). Subsequently, in 2016, the CJEU prohibited Member States from maintaining national data retention regimes if they entail a general and indiscriminate retention of data (see eucrim 4/2016, 164).

Recently, several requests for preliminary rulings were submitted to the CJEU by Member States' supreme or constitutional courts (by Belgium, France, and Estonia). They seek clarification on the limits of retention of e-communication data in view of Art. 15 of the EU's e-privacy Directive 2002/58/EC (cf. case C-520/18; case C-511/18; and case C-746/18). The CJEU will therefore have new opportunities to shape its case law in the field of data retention. (TW)

EDPS Criticises Commission Interoperability Plans by ETIAS

The European Data Protection Supervisor (EDPS) criticised the way the European Commission prepares the interconnection between the European Travel Information and Authorisation System (ETIAS) established in late 2018 (see eucrim 2/2018, 82/84) and the other four EU information systems, i.e., the SIS, ECRIS-TCN, VIS, and EES. On 13 March 2019, the EDPS commented on two Commission proposals presented on 7 January 2019 that changed regulations of the information systems in order to make them ready for interoperability with ETIAS.

The EDPS disagrees with the Commission's stance that the proposals only contain "limited technical adjustments." The EDPS believes that the Commission proposals do not sufficiently protect the purpose limitation principle, especially as regards interconnectivity with the ECRIS-TCN. The ECRIS-TCN stands for the reform of the European Criminal Record System, which will also include information on convicted third-country nationals and stateless persons. The Council and the European Parliament already reached agreement on the new rules, which are currently being formally finalised.

The EDPS recalls that ECRIS-TCN contains very sensitive data and is a tool to support judicial cooperation. Using it

for border management purposes would entail a major change of the system's purpose as defined in the constituent legal act (as currently agreed). If the EU pushes through the Commission proposal, this would mean a "function creep." This means that the use of a system or database is gradually extended beyond the purpose for which it was originally intended. The EDPS is concerned about this trend. He calls on the Commission to carry out a proper data protection assessment of its proposals – to be conducted in full transparency. (TW)

Victim Protection

EP and Council Agree on Directive Protecting Whistleblowers

The European Parliament and the Council reached a compromise on new EU legislation as regards the protection of whistleblowers. The initiative for a directive that aims to lay down uniform minimum standards for the protection of persons who report unlawful activities or abuse of EU legislation goes back to a Commission proposal of 23 April 2018 (see eucrim 1/2018, 27; for the debate, see eucrim 3/2018, 157–159).

The directive applies to a wide range of areas, including:

- Public procurement;
- Financial services;
- Money laundering;
- Product and transport safety;
- Nuclear safety;
- Public health;
- Consumer and data protection.

Which rules should be established in view of the reporting channels was a main point of discussion up to the last moment. Although the majority of Member States favoured a strict three-tiered approach, which included the obligation for whistleblowers to use internal reporting channels first, the European Parliament could push through its flexible approach. Accordingly, whistleblowers are "encouraged" to use internal channels before resorting to external reporting. They are not obliged to do so, however, particularly if the offence cannot be effectively remedied internally or if the reporting person considers that there is a risk of retaliation. Whistleblowers who disclose information publicly are also protected if no appropriate action was taken in response to their initial report or if they believe there is an imminent danger to the public interest or a risk of retaliation.

To meet demands from lawyers' organisations, it was clarified that the Directive does not affect the protection of confidentiality of communications between lawyers and their clients.

Compared to the Commission proposal, further important amendments relate to safeguards against retaliation. Accordingly, the scope of the Directive has been extended to facilitators and to third persons connected with reporting persons who may suffer retaliation in a work-related context, such as colleagues or relatives.

Member States will be obliged to guarantee whistleblowers access to comprehensive and independent information. Whistleblowers must also be able to obtain advice on available procedures and remedies free of charge as well as legal aid during proceedings. During legal proceedings, they may also receive financial and psychological support.

The new EU legislation on the protection of whistleblowers must now be formally adopted in the Council and will undergo linguistic review before publication in the Official Journal. Once it enters into force, Member States will have two years to implement the Directive into their national legislation. (TW)

Journalists Call for Drop of Tiered Reporting Approach in Draft Whistleblowers Directive

On 17 January 2019 – on the eve of the final deliberations in the Council that led to the adoption of its general approach on the directive on the protection of whistleblowers – the European Federation of Journalists (EFJ) re-published an open letter that calls on a robust protection for persons choosing public reporting of unlawful or wrongful acts.

The letter, which was co-signed by four other European media associations, criticises the Commission's proposal of April 2018 (see eucrim 1/2018, 27, and *G. Georgiadou*, eucrim 3/2018, 166) for unsatisfactorily protecting whistleblowers who exercise their right to freedom of expression. The EFJ rebuffs the tiered approach and the order of priority between internal and external channels. Investigative journalists would fail to work properly.

According to the letter, "such layered administrative burdens which fall on the whistleblower would unavoidably have a deterrent effect on the latter and would *de facto* act as an obstacle for the whistleblower to report to the media. This would have a negative impact on media freedom in Europe and on the citizens' fundamental right to receive and impart information, as guaranteed by the European Charter of Fundamental Rights."

The drop of the three-tiered approach is one of the most controversially discussed issues, not only among the EU institutions, but also among civil society stakeholders (see further eucrim 3/2018, 157–159) (TW).

Special Advisor Recommends New Strategy for EU Victims' Rights

Victims still face many difficulties when accessing justice and compensation. The difficulties are often due to a lack of information, insufficient support, and overly restrictive eligibility criteria or procedural hurdles. For persons who become victims of crime when travelling to another EU country, it can be even more difficult to receive compensation. These statements have been included in the report "Strengthening Victims' Rights: From Compensation to Reparation – For a new EU Victims' rights strategy 2020–2025." The report was drafted by former Belgian Vice-Prime Minister *Joëlle Miquet*, who was appointed Spe-

cial Advisor to the President of the European Commission *Jean-Claude Juncker* on compensation for victims of crime.

The report was presented on 11 March 2019 – the 15th Remembrance Day for Victims of Terrorism. It takes a holistic approach to compensation, i.e., it is not limited to the pecuniary aspects of compensation or the compensation procedure, but also tackles the reasons why victims have difficulties in claiming compensation.

The report first carries out a problem analysis, which is grouped into seven thematic chapters:

- Lack of/Access to information and to guidance;
- State compensation;
- Offender compensation;
- Procedural obstacles (length of procedures, complexity, costs);
- Cross-border and international victimisation;
- Free support services;
- Insurance.

The report also dedicates a chapter to the specific needs and problems of specific categories of victims, i.e., victims of terrorism, trafficking in human beings, and gender violence.

Miquet also takes stock of numerous best practices in terms of victims' rights and compensation at the national and EU levels. She points out that a future EU strategy on victims' rights should build on these achievements; however, best rules are only as good as their implementation and application in practice.

The Special Adviser calls on the EU to set up a new victims' rights strategy to tackle the identified problems in a holistic manner: first, immediate practical measures without changing EU legislation and, second, recommendations requiring legislative EU changes.

The report advocates this strategy, which is composed of 41 detailed recommendations around six thematic blocks:

- Better cooperation;
- Training;
- Information;
- State compensation;
- Offender compensation;
- Support services.

In conclusion, *Miquet* calls for swift action in order to reaffirm and reinforce the EU and national commitments strengthening victims' rights. It is important "to show and prove to European citizens that they are living in a Humanistic Europe that protects, cares, repairs, connects, supports and offers a new beginning for everybody."

The Commission will now assess the recommendations and examine whether measures should be taken at the national and European levels to improve victims' access to justice and compensation. (TW)

FRA Reports on Victims' Rights

At the end of April 2019, FRA published a set of four reports on justice for victims of violent crimes. The set of reports deals with access to justice from four different perspectives:

- Victims' rights as a standard of criminal justice;
- Justice in criminal proceedings;
- Sanctions;
- Justice for women who are victims of partner violence.

The reports are based on conversations with victims, workers at victim support organisations, police officers, attorneys, prosecutors, and judges in Austria, France, Germany, the Netherlands, Poland, Portugal, and the UK. They aim at providing practical guidance for policymakers on how to improve the help for victims.

Key recommendations of the reports include the following:

- Provide for more effective and comprehensive backing to address the piecemeal approach to support. This can be achieved through better coordination between the police and support services in order to enable swift and effective referrals. Member States are called on to provide adequate staffing and funding for support services, including free legal aid, counselling, and advice on victims' rights.
- Better protection during court proceedings, i.e., through measures to separate offenders and victims during proceedings in order to prevent further trauma.
- Women who fear of violence from their partners should receive greater police protection, i.e., through the systematic use of barring and court orders.
- Victims should be better compensated for suffering endured and better informed about their rights to compensation. Training for judges should include the importance of compensation as part of the sentencing.
- Offenders should receive rehabilitation measures, such as anti-violence training, probation, and victim-offender mediation. These measures would also benefit society as a whole, as they would help prevent further violence and make offenders more accountable for their actions.
- Special training should be offered to the judiciary and to the police in order to encourage understanding and empathy when dealing with victims and, consequently, to better recognise victims' rights.
- Healthcare providers should be trained to better identify and act on incidents of abuse. The police should be educated on the need to intervene in order to prevent women from further suffering at the hands of their partners.

When presenting the report, FRA Director *Michael O'Flaherty* stated that too many victims of violent crime are not involved in criminal proceedings. More efforts should also be taken to avoid further victimisation. (CR)

AG: New Examination of Victim of Crime Possible if Judges' Bench Changed

Victims of crime may give evidence before the criminal court again if it has a new composition. This is the main conclusion of Advocate General *Yves Bot* in his opinion of 14 March 2019 in case C-38/18 (*criminal proceedings against Massimo Gambino and Shpe-*

tim Hyka). The opinion is not yet available in English.

In the criminal proceedings before the referring Tribunale di Bari, Italy, the hearing of the victim of crime as a witness had to be carried out a second time because one of the three judges was replaced by another judge after the first examination. The defence counsel of the accused persons did not consent to the court reading the written record of the oral evidence previously given by that victim. According to the Italian Code of Procedure, a new examination of the victim as a witness is necessary in this case, in order to maintain the principle of presenting the evidence directly to the judges who decide the case.

The question arose as to whether these provisions are in line with Arts. 16, 18, and 20 lit. b) of Directive 2012/29/EU. These provisions oblige Member States to protect victims of crime from secondary or repeated victimisation and emotional/psychological harm, which includes the obligation to keep questioning to a minimum.

According to AG *Bot*, the provisions must be applied on a case-by-case basis. The competent national authorities must carry out a personalised evaluation. Since the victim was of age and there were no indications for an undue burden, the principle that evidence must be directly presented to the judges deciding the case and the principle of fair trial (on the basis of Arts. 48(2) and 47(2) CFR) takes precedence. Therefore, a new examination of the victim of crime may be admissible. (TW)

Freezing of Assets

CJEU: Executing MS May Impose Imprisonment for Non-Execution of Foreign Confiscation Order

Can a Member State apply a term of imprisonment pending payments, in order to execute a confiscation order adopted in another EU Member State? This was the main question with which the CJEU dealt in the case C-97/18 (*ET*). The Court's judgment is based on a reference for preliminary ruling from the Rechtbank Noord-Nederland (District Court, Northern Region, Netherlands) and concerned the interpretation of Art. 12 of the Framework Decision (FD) 2006/783/JHA on the application of the mutual recognition principle to confiscation orders.

In the case at issue, the Netherlands took over the enforcement of a confiscation order that was imposed on ET by the Court of Appeal, Antwerp, Belgium. The Dutch public prosecutor sought leave to enforce a term of imprisonment against ET since over €650,000 out of the ordered €800,000 were outstanding and ET was suspected of invisible financial flaws. ET argued that the application for a term of imprisonment is unlawful and in contrast with Art. 7(1) ECHR, Art. 49(1) CFR.

The referring court indeed confirmed that the measure of imprisonment as that at issue is considered a penalty within the meaning of Art. 7 ECHR in the case law of the Supreme Court of the Netherlands. Therefore, the Rechtbank Noord-Nederland first harbours doubts whether the Dutch executing authorities may apply the measure of imprisonment pending payment within the scheme of the EU's FD 2006/783/JHA. Second, the court asks whether the application of the measure necessitates that the issuing state also makes provision for the possibility of applying a term of imprisonment pending payment.

As regards the first question, the CJEU states that Art. 12(1) and (4) of the FD posits that, as a general rule, it is for the execution State's competent authorities to decide, in accordance with the law of that State, the manner in which the execution is to be carried out and the most adequate measures to execute the confiscation order. However, as a special rule, in accordance with para. 4, the prior agreement of the issuing State is required if the measure envisaged by the executing State were to appear to replace that order. It must therefore be examined whether these rules preclude a measure as that in question.

In this context, the CJEU observed that the term of imprisonment is applied as a leverage against a person who is not willing, but capable to pay the amount owed. The person concerned may, at any time, be freed from imprisonment if he/she pays the debt; furthermore, the measures is limited in time and duration depends, *inter alia*, on partial payments possibly made. The adoption of such imprisonment is neither an alternative to the order nor an additional sanction. Consequently, it does not require the prior consent of the issuing State. It is completely up to the executing State how to pursue the objectives of the FD.

The classification of the terms of imprisonment as a "penalty", within the meaning of Art. 7 ECHR, by the Dutch Supreme Court has no influence on the competent authorities to implement all the necessary measures for the execution of foreign confiscation orders.

As to the second question, the CJEU briefly noted that it follows from Art. 12(1) of the FD that the legislation of the issuing State has no bearing on the application of the measure in question in the executing State. (TW)

Report on Asset Recovery Casework

In February 2019, Eurojust published a report on its casework in asset recovery with the following overview:

- The main legal and practical issues encountered by Eurojust in its asset recovery casework;
- The support provided by Eurojust during the asset recovery process;
- The main judicial cooperation instruments and tools used;
- The best practice identified.

It aims at assisting competent judicial authorities in the EU Member States in effectively recovering criminal assets and in contributing to the fight against transnational crime. Based on an analysis of cases addressing asset recovery issues registered at Eurojust between

1 January 2014 and 31 March 2018, the report identifies the main practical benefits of asset tracing, asset freezing and confiscation, asset disposal, and Eurojust's support.

The benefits of asset tracing include using specialised forensic accountants, taking a multi-disciplinary approach, and raising awareness about the support offered by Asset Recovery Offices and Financial Intelligence Units.

With regard to asset freezing and confiscation, the report identifies benefits such as early consultation between the authorities in the Member States, a comprehensive understanding of the EU- and international legal instruments, and an understanding of the distinctions in the ultimate confiscation instrument to be applied.

In relation to asset disposal, the report recommends anticipating potential causes for delay, anticipating requirements such as provisions for compensation, and considering, if possible, the early sale of assets.

Lastly, looking at Eurojust's support, the report identifies several benefits, for instance the coordination of a joint investigative strategy and intelligence activities, the exchange of relevant information, the provision of a channel of communication, the coordination of the transmission and execution of Letters of Request, freezing and confiscation orders, and assistance with drafting these requests and orders. (CR)

Cooperation

Police Cooperation

Debate on Home Affairs Progress

At the JHA Council meeting on 7 March 2019, the Home Affairs Ministers of the EU Member States discussed achievements made in the last five years in the area of home affairs and the challenges ahead. The debate must be seen in the context of the preparations for a new Strategic Agenda which is to be adopted by the European Council at the summit in June 2019. Matters raised included the need for more integration between different policy areas, the development of cooperation and partnerships with third countries to address common challenges and the implementation of the legislation agreed. (TW)

EP Study: Possible EU Action Against Misuse of Interpol Red Notice System

In February 2019, the European Parliament published a study that examined the abuse by some states of the Interpol's notice system to persecute national human rights defenders, civil society activists and critical journalists in violation of international standards of human rights. The study entitled "Misuse of Interpol's Red Notices and impact on human rights – recent developments" was requested by the EP's Subcommittee on Human Rights (DROI).

The authors of the study shed light on the current situation and recent trends after Interpol has introduced reforms to its legal and procedural framework in vetting red notices and diffusions in 2015. The reform included a new refugee policy, a strengthened review process of requests for red notices and diffusions in Interpol's General Secretariat (GS), and the set-up of rules to govern the new mandates of the Commission for the Control of Interpol's Files (CCF).

The study does, in particular, the following:

- Providing an overview of reported abuses and assessing their nature;
- Describing the recent reforms undertaken by Interpol and assessing their implementation so far;
- Looking at the responses of EU and Member States;
- On this basis, identifying practices that are still in need of reform and recommending strategic activities, which the EU and its Member States could advocate to prevent the abuse of Interpol and its mechanisms.

The study is based on written material that focuses on practices after the 2015 reforms. Furthermore, interviews were conducted with Interpol, the European Commission, and relevant organisations.

The study acknowledges that the reforms of 2015 have improved the situation, however, abuses of the Interpol system against individuals, including refugees, still continue. There is still a lack of established rules and procedures to govern the vetting process and the adherence to Interpol Constitution. A main issue of concern is that information about red notices and diffusions is not timely updated. This is mainly due to the Interpol system which is based on national databases with national authorities under national jurisdiction, and therefore a lack of any influence from central entities.

Another challenge remains transparency, both at the individual and the organisational level. Individuals have limited access to the rules and procedures the GS and the CCF apply in the evaluation process. Member countries and other international organisations have little access to information about the overall handling of red notices and diffusions. Concrete data on the countries making requests, the number of accepted/refused requests, the grounds for refusals, etc. do not exist. Hence, according to the authors, "it is not possible to evaluate, even on the simplest level, the quality of the vetting process..."

As regards possible EU action to remedy the current problems of abuses, the study recommends, *inter alia*, the following:

- EU institutions and EU Member States should take action that Interpol further develops the legal framework and its applicability for the GS, the CCF and the National Central Bureaus (NCBs);
- EU Member States should ensure that Interpol fully implements the reforms commenced in 2015;
- EU Member States should engage more actively in strengthening the accountability of the GS, CCF, and NCBs

to control the content and updates of red notices;
- Further steps are needed to fully implement the refugee policy;
- An independent redress to CCF decisions is needed, e.g. by an ombudsman;
- The EU could fund further projects specifically aimed to improve the clarity and transparency of the processing and screening of red notices and diffusions in order to avoid human rights violations;
- The EU could engage in bilateral initiatives with the member countries outside of the EU that cause the biggest problems to an accountable Interpol system, e.g. through a new development programme to raise the human rights and rule of law capacity in the international cooperation in criminal matters;
- The EU should also address the individuals affected by wrongful red notices or diffusions, e.g. by supporting relevant NGOs that engage in deletion of the persons from the system;
- The EU Institutions, bodies and EU Member States should ensure further transparency concerning the activities of police authorities and their relationship with international organisations and third countries in dealing with red notices.

Finally, the Commission is called on to continue the monitoring of the EU Member States' compliance with the principle of non-refoulement and EU data protection rules. (TW)

Customs Cooperation

Council Conclusions on Customs Risk Management

At the meeting on 8 January 2019, the Council (General Affairs) approved conclusions on the Commission's second progress report on the Implementation of the EU Strategy and Action Plan for Customs Risk Management.

The Council, *inter alia*, welcomed the participation of customs administrations in security-related activities, the improvement in cooperation between customs and trade, and the improved exchange of specific customs information between customs authorities in the EU and third countries (including the establishment of a framework for the structured exchange of information with third countries).

Notwithstanding, the partnership of customs with trade as well as cooperation with international partners still need to be further explored and enhanced. The cooperation of law enforcement authorities in interlinking customs controls and risk management, on the one hand, and fraud/crime prevention and detection/investigation measures, on the other, need to be constantly evaluated.

The conclusions address numerous recommendations to the Member States and the Commission (each within their respective competence), including *inter alia*:
- To utilise all available resources to accelerate the implementation of essential IT systems;
- To increase the efficiency and effectiveness of customs controls based on risk analysis;
- To improve synergies between customs and other law enforcement authorities in the area of organised crime, security, and fight against terrorism, both at the national and EU levels;
- To further explore the technical, operational, and legal aspects of interoperability of the security and border management systems with customs systems;
- To enhance the exchange of information related to risks between Member States and between Member States and third countries.

The Commission has been called on to develop an efficient reporting mechanism – in close cooperation with the Member States – to measure the impact of outcomes/results of specific actions deriving from the EU Strategy and Action Plan. In addition, a new working group is to define the indicators that will facilitate the implementation of the EU Strategy and Action Plan. (TW)

European Arrest Warrant

CJEU: German Public Prosecution Office Is Not a "Judicial Authority" in the EAW Context

spot light

German public prosecution offices may no longer issue European Arrest Warrants. With this thunderbolt, the CJEU (Grand Chamber) answered two references for a preliminary ruling from Irish courts.

➤ *Background*

In the Joined Cases C-508/18 (*OG*) and C-82/19 PPU (*PI*), the CJEU further developed its case law on the concept of "issuing judicial authority" within the meaning of Framework Decision 2002/584/JHA on the European Arrest Warrant (FD EAW). The case law started with the rulings of 10 November 2016 in cases C-452/16 PPU (*Poltorak*), C-477/16 (*Kovalkovas*), and C-453/16 (*Özcelik*) – see eucrim 4/2016, 165–167. In these cases, the CJEU clarified that police services and ministries of justice are not an "issuing judicial authority" in the sense of Arts. 1(1) and 6(1) FD EAW. Confirmation by a prosecutor of an EAW that had been previously issued by a police authority can, however, be considered a "judicial decision" in accordance with Art. 8(1c) FD EAW.

In proceedings before Irish courts, the question was then raised as to whether public prosecution offices guarantee sufficient independence to be viewed as a "judicial authority" in the sense as required by the aforementioned case law. In addition to the questions relating to the German public prosecution service, the Irish Supreme Court also brought up a preliminary ruling concerning the Lithuanian Prosecutor General's Office, which has the capacity to issue EAWs in Lithuania (case C-509/18, see separate eucrim news).

➤ *Facts of the Joined Cases*

As regards the preliminary ruling proceedings on the German public prosecution offices, defendants whose surrender from Ireland had been requested by the prosecution services of Lübeck

(case C-508/18) and Zwickau (case C-82/19 PPU) argued that, in fact, no "judicial authority" within the meaning of Art. 6(1) FD EAW was involved in the issuance of the European Arrest Warrants. The reasoning is as follows:

- German public prosecution offices are only entitled to execute a national arrest warrant issued by a judge or court;
- German public prosecution offices do not enjoy an autonomous and independent status, but are subject to an administrative hierarchy headed by the Minster for Justice.

Indeed, under German law, German public prosecution offices are commonly designated as the competent authority to issue European Arrest Warrants, especially those for the purpose of prosecution. Furthermore, there is a relationship between the public prosecutor's offices and the executive in Germany. In particular, public prosecutors are subject to the "external power" of the ministers of justice of the relevant federal state (*Land*) to issue instructions (*externes Weisungsrecht*). Germany argued, however, that this power is exercised only as an exception and that no instructions had been issued in the present case.

➤ *Questions Referred*

Notwithstanding, the referring Irish Supreme Court and the Irish High Court cast doubt as to whether the structure and powers of the German public prosecution offices meet the so-called independence and administering of justice tests established by the CJEU in the "trias" rulings *Poltorak*, *Kovalkovas*, and *Özcelik*. They mainly want to know which criteria and parameters govern assessment of the term "independence" within the context of the FD EAW. If independence from the executive can be affirmed, the courts also ask whether a public prosecutor, who is confined to

- Initiating and conducting investigations and assuring that such investigations are conducted objectively and lawfully;
- The issuing of indictments;
- Executing judicial decisions and conducting the prosecution of criminal offences; and who
- Does not issue national warrants;
- May not perform judicial functions,

can be considered a "judicial authority" for the purposes of Art. 6(1) FD EAW.

➤ *Ruling of the CJEU*

In its ruling of 27 May 2019, the CJEU first clarifies that the multiple questions referred to can be condensed to the essential question of "whether the concept of an 'issuing judicial authority', within the meaning of Art. 6(1) [FD 2002/584], must be interpreted as including the public prosecutors' offices of a Member State which are responsible for the prosecution of criminal offences and are subordinate to a body of the executive of that Member State, such as a Minister for Justice, and may be subject, directly or indirectly, to directions or instructions in a specific case from that body in connection with the adoption of a decision to issue a European arrest warrant."

In accordance with the principle of procedural autonomy, the CJEU first reiterates that, although Member States may designate, in their national law, the "judicial authority" competent to issue EAWs, the meaning and scope of that term cannot be left to the assessment of each Member State. Therefore, the term "judicial authority" requires an autonomous and uniform interpretation throughout the EU, taking into account the wording, context, and objective of the FD EAW.

The concept of an "issuing judicial authority" must cumulatively meet two criteria:

- The authority participates in the *administration of criminal justice* in an EU Member State (as distinct from, *inter alia*, ministries or police services, which are part of the executive);
- The authority responsible for issuing an EAW must *act independently* in the execution of its functions (even if the EAW is based on a national arrest warrant issued by a judge or court).

The CJEU held that the first criterion is fulfilled: a public prosecution office, such as the German one, which is competent to prosecute a person for a criminal offence and bring that person before a court, must be regarded as "participating in the administration of criminal justice."

As regards the second criterion, the judges in Luxembourg focused on the protection of the procedural and fundamental rights of the person sought. Accordingly, the EAW system involves a dual level of protection: the first level provides judicial protection for a national decision, such as a national arrest warrant; the second level affords protection when a European Arrest Warrant is issued (possibly shortly after the adoption of the national judicial decision). At this second level, the judicial authority "must review, in particular, observance of the conditions necessary for the issuing of the EAW and examine the proportionality of the EAW." As a result, the Member States must guarantee that the "issuing judicial authority," within the meaning of Art. 6(1) FD EAW, must meet the following capacities:

- Exercising its responsibilities objectively;
- Taking into account all incriminatory and exculpatory evidence;
- Not being exposed to the risk that its decision-making power is subject to external directions or instructions, in particular from the executive.

In other words: the issuing Member State must assure "that it is beyond doubt that the decision to issue a European arrest warrant lies with that authority and not, ultimately, with the executive."

In addition: if the authority to which the Member State confers the competence to issue EAWs is not itself a court, the decision to issue an EAW – and, in particular, the proportionality of such decision – must be subject to court proceedings, "which meet in full the requirements inherent in effective judicial protection."

In view of the established parameters, the CJEU stated that the German pub-

lic prosecution offices may, in a given case, be subject to instruction from the Minister for Justice of the relevant *Land*. Hence, they are not free from (direct) political influence. As a consequence, a criterion of the independence test as described above is not fulfilled.

The Luxembourg judges rejected the arguments by the German government that German law includes several safeguards that circumscribe the ministers' power to issue instructions, so that situations in which this power could be exercised are extremely rare. According to the CJEU, the abstract existence of these powers already suffices, namely that the German public prosecution offices cannot be subsumed under the autonomous notion of "judicial authority."

➤ *Put in Focus*

The CJEU's Grand Chamber ruling will have considerable consequences on the German practice. Germany is one of the EU Member States that issues the most EAWs yearly (in 2018 and 2017, over 3700 EAWs were issued via the SIS). The vast majority of EAWs were issued by the public prosecution services. All issued EAWs have now become invalid and need to be reissued. At the moment, it is not clear, however, how the issuance of EAWs will be organised in the future. As statements in an article on the judgment in the "Legal Tribune Online" reveal, there are several possibilities:

- EAWs may be issued by the judge at the local court who issues national arrest warrants;
- EAWs may be issued by the trial court, or the court where a criminal case is currently pending, or a chamber that will execute a possible conviction.

In any event, the German law must be amended in the near future.

Probably like many other Member States, Germany considered the European Arrest Warrant framework to not only include a request for extradition/surrender, but that it is also an instrument for searching persons. This latter aspect now seems to have been pushed back by the CJEU, which made clear that the European Arrest Warrant can be the basis for depriving a person of his/her liberty. Therefore, judicial oversight and control must be strong during the issuing phase of an EAW.

Still, questions remain open. The consequences of the CJEU's statements are not yet fully clear. The result of the joined cases C-508/18 and C-82/19 PPU was also shared by the Advocate-General *Manuel Campos Sánchez-Bordona* in his opinion of 30 April 2019. The AG, went a step further, however, by concluding that – according to his view – only a judge or a court is capable of properly issuing an EAW. Prosecution services should only be entitled to issue EAWs in exceptional circumstances, e.g., in urgent cases, in accordance with the national law of a Member State. Restricting the competence to issue an EAW to judges/courts avoids verification of institutional and functional autonomy in each individual EAW case. In its judgments C-508/19 and C-82/19 PPU, the CJEU does not seem to draw this conclusion, even in comparison to the decision regarding the Court's finding in case C-509/19 on the Lithuanian General Prosecution Service. This is mainly because, in the "German case," the CJEU focuses on whether prosecution services are exposed to the risk of being subject (directly or indirectly) to directions or instructions from the executive (such as ministers). In the "Lithuanian case," the CJEU does not fully exclude prosecution services from the concept of "issuing judicial authorities." This means that executing authorities will have to examine the status of the prosecution services in EAW cases and carry out individual assessments in the future. Therefore, uncertainties for legal practitioners executing EAWs will remain, which may not only delay surrender, but also trigger similar references.

Coming back to Germany: the ultimate question is whether the structure of the German public prosecution offices, with their embedding in the executive branch, must be overhauled. The abolition of external power for the ministers of justice to give instructions is a recurring request which has gained new momentum with the present CJEU judgment. (TW)

Lithuanian Prosecutor General Included in the Concept of "Judicial Authority" in the FD EAW

The Prosecutor General of Lithuania can be considered a "judicial authority" that can issue European Arrest Warrants, under the condition that his/her decisions are subject to court proceedings fully meeting the requirements inherent to effective judicial protection. It is up to the referring court to determine the latter.

➤ *Context of the Case*

The Grand Chamber of the CJEU concluded this finding in its judgment of 27 May 2019 in case C-509/18 (*PF*). It was rendered in parallel to its judgment of the same day in the joined cases C-508/18 (OG) and C-82/19 PPU (PI) – see separate eucrim news. All cases were referred by Irish courts (case C-509/18 by the Irish Supreme Court); persons requested for surrender via European Arrest Warrants claimed that the issuing public prosecution offices are not competent to issue EAWs because they lack the independence required to be a "judicial authority" within the meaning of Art. 6(1) of Framework Decision 2002/584/JHA on the European Arrest Warrant (FD EAW).

The cases build on the case law in cases C-452/16 PPU (*Poltorak*), C-477/16 (*Kovalkovas*), and C-453/16 (*Özcelik*) – see eucrim 4/2016, 165–167 – in which the CJEU first established several criteria according to which the authority may be regarded as "judicial" within the EAW scheme. The referring Irish courts doubted whether the so-called independence and administering of criminal justice tests – as described in the aforementioned case-law – are fulfilled if public prosecutors from other EU Member States issue EAWs on the basis of the FD.

Whereas the question in the joined cases C-508/18 and C-82/19 PPU relate to the German public prosecution office, the present case C-509/18 concerns the Prosecutor General of Lithuania.

➤ *Facts of the Case*

In the case at issue, the Prosecutor General of Lithuania issued a European Arrest Warrant for the surrender of a Lithuanian national PF who was prosecuted for "armed robbery," allegedly committed in 2012. PF challenged the validity of the EAW on the grounds, *inter alia*, that the Prosecutor General is not an "issuing judicial authority" within the meaning of Art. 6(1) FD EAW. He argued that, according to the case law of the Lithuanian constitutional court, a public prosecutor is not responsible for the administration of justice. In the appeal proceedings against execution of the EAW, the Irish Supreme Court followed this argumentation and identified that the CJEU's case law as regards the definition of "judicial authority" pursuant to Art. 6(1) FD EAW is incomplete. The Irish Supreme Court mainly asked the CJEU for more concrete criteria that allow the national courts to determine the "judicial authority" for the purposes of the FD EAW.

➤ *The CJEU's Ruling*

The CJEU first clarified that the essential question in the given case is whether the Prosecutor General of a Member State can be included in the concept of an "issuing judicial authority" within the meaning of Art. 6(1) FD EAW. In contrast to the parallel cases C-508/18 and C-82/19 concerning the German public prosecution office, the CJEU highlighted that the following characteristics of the Lithuanian Prosecutor General must be taken into account:

- Institutionally independence from the judiciary;
- Responsibility for conducting criminal prosecutions;
- Independence from the executive.

The judges in Luxembourg then deliberated the criteria and parameters for determining the "issuing judicial authority" as established in the joined cases C-508/18 and C-82/19. In particular, the concept requires an autonomous and uniform interpretation at the EU level.

First of all, it must be established whether the authority at issue is "participating in the administration of criminal justice" in a Member State. In this context, it follows from the FD EAW that the concept of "judicial authority" not only refers to judges and courts, but may also encompass other authorities involved in the criminal proceedings. These authorities must, however, be capable of adopting decisions in relation to conducting criminal proceedings. For example, the Prosecutor General in Lithuania is capable of being regarded as participating in the administration of criminal justice in the Member State in question.

Secondly, if the EAW was not issued by a judge or court, the competent authority must act independently. In particular, it must have sufficient power to protect the individual's procedural and fundamental rights when issuing an EAW. Therefore, the issuing authority must have the following capacities:

- Exercise its functions objectively;
- Take into account all incriminatory and exculpatory evidence;
- Not be exposed to the risk that its decision-making powers are subject to external directions/instructions, in particular from the executive.

In addition, sufficient protection means that the decision on issuing a European Arrest Warrant meets "the requirements inherent in effective judicial protection" (if the decision was not adopted by a judge or a court).

The CJEU found that the legal position of the Prosecutor General of Lithuania safeguards not only the objectivity of his role, but also affords him a guarantee of independence from the executive in connection with the issuing of an EAW. The CJEU could not, however, ascertain whether a decision of the Prosecutor General to issue an EAW may be the subject of court proceedings "which meet in full the requirements inherent in effective judicial protection." This is ultimately for the referring court to determine.

➤ *Put in Focus*

Together with the judgment in the joined cases C-508/18 and C-82/19 PPU, the CJEU supplements its case law as to the extent to which the executing judicial authority can be sure that an EAW has been issued by a "judicial authority" as required by the FD EAW. Both judgments must be read together, and the previous judgments in the aforementioned cases decided in 2016 (*Poltorak*, *Kovalkovas*, and *Özcelik*) must also be taken into account. In further clarifying the criteria of the concept of "judicial authority," the CJEU's approach does, however, require the executing authority to assess the status of public prosecution offices in each individual Member State if they issue EAWs. This not only leads to uncertainties, but may also delay surrender.

In its opinion of 30 April 2019, Advocate-General *Manuel Campos Sánchez-Bordona* tried to avoid this consequence. He proposed excluding the institution of public prosecutors' offices from the concept of "issuing judicial authority." He argued that independence can only be recognised for the judiciary, but not for the public prosecutor's office. The Grand Chamber disagreed with this view in case C-509/18 (TW).

CJEU: Relationship Between Time Limits in the FD EAW and Surrender Detention

In its judgment of 12 February 2019, the CJEU dealt with the implication of non-compliance with the time limits for the decision to execute a European Arrest Warrant on maintaining the requested person's extradition detention. The CJEU ultimately had to decide whether the Dutch law implementing Framework Decision 2002/584/JHA on the European Arrest Warrant (FD EAW) and the case law of the Amsterdam courts could be upheld against Art. 6 of the Charter of Fundamental Rights of the EU (CFR). The case is referred to as C-492/18 PPU (*TC*).

➤ *Background of the Case and Facts*

The reference for a preliminary ruling was made by the Rechtbank Amsterdam (District Court, Amsterdam, Netherlands). According to the Rechtbank, situations may occur in which it is not able to maintain the time limits as provided for in Art. 17 FD EAW. The provision stipulates that a final decision on execution of the EAW should be taken by 90 days after the arrest of the requested person at the latest. This deadline cannot be met if a preliminary ruling must be made to the CJEU or if the court assesses possible inhuman or degrading treatment in the issuing Member State in line with the CJEU's judgment in *Aranyosi and Căldăraru* (cases C-104/15 and C-659/15 PPU).

A similar situation occurred in the case at issue, when the Rechtbank Amsterdam stayed the execution of the European Arrest Warrant issued by the United Kingdom against TC, a British national, because the Amsterdam court wanted to wait for the CJEU's response in case C-327/18 (*RO*). In this preliminary ruling procedure, the CJEU had to decide on the impact of the UK's notification of its intention to withdraw from the EU on the execution of an EAW issued by the UK authorities (see eucrim 2/2018, 102–103).

The Dutch legislator, however, considered the time limits in the FD EAW to be in favour of the individual. As a consequence, detention of the requested person must be suspended,if the 90-day period for adopting a final decision on execution of the EAW has expired (Art. 22(4) of the Overleveringswet [OLW − Law on the surrender of sentenced persons]).

The referring court further noted that both the court itself and also the appeal court in Amsterdam (Gerechtshof Amsterdam) had developed case law that avoids the strict legal consequence of Art. 22(4). This case law aims at interpreting the Dutch law in conformity with the FD EAW. However, the two courts take different approaches to determining the suspension of the time period in Art. 22(4), even though both approaches have brought about the same results in practice.

In the present case, the Rechtbank Amsterdam followed its approach and suspended the decision period until delivery of the judgment in RO. The Rechtbank also remarks that it was unable to equally suspend detention pending surrender because there was a very serious risk of TC absconding, which could not be reduced to acceptable levels.

➤ *Legal Questions at Issue*

Against this background, the Rechtbank Amsterdam sought clarification from the CJEU as to whether Art. 22(4) OLW, laying down a general and unconditional obligation to release a requested person after the 90-day period has elapsed, is in line with the concept of an effective surrender as set up by the FD EAW. In addition, the question was raised as to whether Art. 6 CFR, which guarantees a person's right to liberty, precludes national case law allowing suspension of the 90-day period in the aforementioned situations.

➤ *Ruling of the CJEU*

As regards the first question, the CJEU indicated that the Dutch legislator had apparently a misunderstanding of the provisions in the FD EAW. Neither Art. 12 FD EAW, which gives the executing authority the power to take decisions on whether a requested person must be arrested or remain in detention, nor any other provision of the FD EAW requires the release of that person *a fortiori* if the time limits stipulated in Art. 17 expire. Such an obligation to release the person would ultimately obstruct the attainment of the objectives pursued by the FD EAW, which seeks to build up an effective surrender system within the EU territory.

This effectiveness is especially undermined if, as indicated in the case at issue, the executing authority were to be obliged to carry out a provisional release, even if there is a very serious risk of absconding (which could not be reduced to an acceptable level by the imposition of appropriate measures). The material conditions necessary for the effective surrender would not be able to be maintained. Accordingly, Art. 22(4) OLW is incompatible with the provisions of FD 2002/584.

As regards the second question, the CJEU stated that Art. 12 FD EAW must be interpreted in conformity with Art. 6 CFR. However, this fundamental right to liberty is subject to limitations which in turn must fulfil several conditions, e.g., being proportionate (Art. 52(1) CFR). Since Art. 6 CFR corresponds to Art. 5 ECHR, account must be taken of the relevant interpretation by the ECtHR (Art. 52(3) CFR). In this context, the ECtHR requires not only that any lawful deprivation of liberty must have a basis in national law, but also that this law must be sufficiently accessible, precise, and predictable in its application in order to avoid all risk of arbitrariness.

In applying these parameters, the CJEU found that the given case law of the Rechtbank and Gerechtshof of Amsterdam in making exceptions to Art. 22(4) OLW does not make it possible for the person concerned to clearly and predictably determine the period of his detention. Although the approaches may not entail different results in practice, it cannot be ruled out that these divergences may lead to different periods of continued detention (notably because both courts did not proceed from the same starting point in calculating the suspension period). Furthermore, the differing interpretations cannot exclude that a person must be released even if there is a high risk of absconding – as a result of which conformity with the FD EAW cannot be achieved (see above).

In conclusion, the current practice in the Netherlands of keeping a person in detention beyond the 90-day period infringes Art. 6 CFR.

➤ *Put on Focus*

Although one might first think that the present judgment in TC is intertwined with the special legal situation in the

Netherlands, it confirms the CJEU's approach already established in the *Lanigan* judgment of 16 July 2015 (C-237/15 PPU). Accordingly, time limits as stipulated in the FD EAW are above all addressed to the state authorities. They do not preclude keeping a requested person in custody, even if the total duration for which that person has been held in custody exceeds those time limits. The first premise is to ensure the effectiveness of the surrender. The limit is the CFR, in particular Art. 6 as interpreted in the light of Art. 5 ECHR. The duration of detention cannot be excessive and must reflect the principle of proportionality. If the executing authority is opting for provisional release, it is, however, required to attach any measures it deems necessary to prevent the person concerned from absconding and to ensure that the material conditions necessary for his/her effective surrender remain fulfilled as long as no final decision on the execution of the EAW has been taken. (TW)

AG: Assessment Standards of Detention Conditions in EAW Cases

On 30 April 2019, Advocate General (AG) *Manuel Campos Sánchez-Bordona* presented his opinion in case C-128/18 (*Dumitru-Tudor Dorobantu*). The request for a preliminary ruling was made by the Higher Regional Court (HRC) of Hamburg, Germany, which initially ordered the surrender of Romanian national Mr *Dorobantu* to Romania in respect of offences relating to property and forgery and the use of forged documents.

Mr Dorobantu claimed that surrender to Romania would infringe his fundamental rights, since he would be incarcerated in prisons that do not fulfil the minimum standards of human and non-degrading treatment. The assessment of the referring court as regards detention conditions in Romania, finding that they comply with the standards of Art. 4 CFR, was quashed by the German Federal Constitutional Court (FCC). The FCC demanded that the HRC of Hamburg file a request for preliminary ruling to the CJEU, so that the latter further determine the factors relevant to the assessment of the detention conditions in the issuing State. For the case history, see eucrim 1/2018, 32–33.

Subsequently, the HRC of Hamburg stayed the EAW proceedings and posed several questions to the CJEU. The first block of questions relates to the minimum standards for custodial conditions required under Art. 4 CFR. The second block deals with questions as to which standards are to be used to assess whether custodial conditions comply with EU law and to which extent these standards influence interpretation of the term "real risk" as defined in the leading judgment *Arranyosi and Căldăraru* (see eucrim 1/2016, 16).

The AG first examined the level of review of detention conditions that the executing authority is entitled to carry out within the EAW regime. Secondly, he elaborated on the underlying criteria for review of the detention conditions in the establishment where the person surrendered is likely to be incarcerated.

In conclusion, the AG proposed that the executing judicial authority meet the following obligations:

- Carry out an overall assessment of all the material aspects of the detention that are relevant to the assessment of whether there is a real risk of inhuman or degrading treatment as a result of poor detention conditions;
- Place particular importance on the minimum personal space in the prison cell;
- Take into account the type of cell (single occupancy or multiple occupancy) and the space taken up by furniture (excluding sanitary facilities);
- Examine other material aspects of detention, e.g., layout of the cell, essential services, and infrastructure of the prison, out-of-cell activities, etc., if the cell is 3m² or less, in order to assess compensation for lack of personal space and rebut the presumption of a breach of Art. 4 CFR;
- Take into account the duration and extent of the restriction, the type of prison, and the prison regime, when assessing the various factors.

Ultimately, the AG concluded that legislative and structural measures for improvement of the execution of sentences in the issuing EU Member State cannot, as such, mitigate the real risk of inhuman and degrading treatment to which the person surrendered would be exposed. Furthermore, the executing judicial authority cannot weigh the individual's guarantee to not be subject to any inhuman or degrading treatment in the sense of Art. 4 CFR against compliance with the principles of mutual trust and mutual recognition and with safeguarding the effectiveness of the European criminal justice system.

After the above-mentioned judgment in *Arranyosi and Căldăraru* and contributions made by the judgment in case C-220/18 PPU (*Generalstaatsanwaltschaft [conditions of detention in Hungary]*, also referred to as "Aranyosi III", see eucrim 2/2018, 103–104), the *Dorobantu* case gives the CJEU a further opportunity to shape the required assurances for respecting the fundamental rights of the person surrendered under a European Arrest Warrant when there are general or systematic deficiencies in the prison system in the issuing EU Member State. (TW)

European Investigation Order

AG: Bulgaria Must Bring Its Law in Line with EIO Directive

If the national legislation of an EU Member State does not provide for legal remedies, by means of which the substantive reasons for an investigative measure requested by a European Investigation Order (EIO), cannot be challenged, this Member State is not entitled to use the EIO instrument.

➤ *Background*

This far-reaching legal ramification was proposed by Advocate General *Yves Bot*

in his opinion of 11 April 2019 in case C-324/17 (*criminal proceedings against Ivan Gavanozov*). Note: At the time of writing, the opinion was not available in English and German.

The case marked the first occasion for the CJEU to interpret Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO DIR). It concerns peculiarities of Bulgarian criminal procedure, and interpretation was requested as regards Art. 14 EIO DIR, which provides *inter alia*:

- Member States shall ensure that legal remedies equivalent to those available in a similar domestic case are applicable to the investigative measures indicated in the EIO (Art. 14(1));
- The substantive reasons for issuing the EIO may be challenged only in an action brought in the issuing State, without prejudice to the guarantees of fundamental rights in the executing State (Art. 14(2));
- "Parties concerned" shall have the possibility to effectively exercise these legal remedies (cf. Art. 14(4)).

➤ *Facts of the Case*

The request for a preliminary ruling was made by the *Spetsializiran nakazatelen sad* (Specialised Criminal Court, Bulgaria) in criminal proceedings against *Ivan Dimov Gavanozov* who was being prosecuted for VAT fraud in Bulgaria. Allegedly, a company and its manager situated in the Czech Republic were involved in the fraud scheme. Hence, the Bulgarian court wished to issue an EIO requesting the Czech authorities to search residential and business premises, seize specific documents, and examine the manager as a witness. However, the Bulgarian court noted that neither the Bulgarian code of criminal procedure nor the law implementing Directive 2014/41 provide for a legal remedy against the adoption of the investigative measures of search and seizure and witness examination. Therefore, the court was also unable to fill in Section J of the EIO form, which refers to the legal remedies in the issuing State.

➤ *Referred Questions*

As a consequence, the Specialised Criminal Court referred three questions to the CJEU:

- Is the Bulgarian legislation, which (directly and indirectly) precludes a challenge to the substantive grounds of a court decision issuing an EIO for a search of premises and the seizure of specific items and allowing examination of a witness, consistent with Art. 14 EIO DIR?
- Does Art. 14(2) EIO DIR grant, in an immediate and direct manner, to a concerned party the right to challenge a court decision issuing an EIO?
- Who is covered by the term "concerned party"?

➤ *The Advocate General's Answers*

As regards the first question, the AG observed that, although Art. 14 EIO DIR only obliges Member States to extend existing legal remedies to the EIO context, it can be deduced from the norm that – "as a play of mirrors" – Member States are also obliged to install legal remedies which enable concerned parties to challenge the substantial grounds for issuing the EIO.

The AG even went a step further. Not only is Bulgarian legislation inconsistent with Art. 14 EIO DIR, but the Bulgarian authorities are also presently not allowed to issue EIOs, i.e., to use the EIO instrument. The AG argued that the principle of mutual trust and recognition is built on a balance between effectively cooperating in criminal matters and guaranteeing an individual's fundamental rights. The respect of fundamental rights, however, cannot be presumed if the issuing State denies legal remedies to the persons concerned by the cooperation. Referring to case law of the ECtHR, the AG further concluded that the current Bulgarian legislation is a "flagrant denial of justice" and that deficiencies must be remedied before the EIO can be used.

As regards the second question, the AG stated that Art. 14(2) EIO DIR does not grant, in a direct and immediate manner, a right to challenge an EIO in favour of the "parties concerned." A direct effect for a legal remedy against an investigative measure cannot be created *ex nihilo*.

By answering the second question in the negative, the third question actually became obsolete. Alternatively, AG *Bot* points out that the notion "concerned parties" must be interpreted autonomously. It also covers persons who are affected by an investigative measure, but are considered a "third party" in the criminal procedure, e.g., the person who occupies the property on which the search and seizure is carried out or the person who is to be examined as a witness. The Union legislator did not exclude the protection of these persons if an EIO is applied (Art. 1(4)). In addition, the "concerned party" in Art. 14(4) EIO DIR includes the person against whom a criminal charge was brought, even though that person was not directly targeted by the measure that collected the evidence. (TW)

Eurojust Meeting Report on European Investigation Order

Eurojust published a report about a two-day meeting on the European Investigation Order (EIO) attended by prosecutors from the EU Member States as well as representatives from EU institutions and academia at Eurojust's premises in the Hague from 19–20 September 2018. The meeting provided a platform for debate in order to discuss potential problems and challenges.

The report gives an overview of the scope, content, form and language, issuing and transmission, recognition and execution, and specific investigation measures of an EIO. Furthermore, it outlines the specific support of EIO actors.

Overall, participants at the meeting concurred that, with the EIO, a standalone legal instrument covering all types of investigative measures (with the exception of JITs) in the field of evidence-gathering within the EU has been established.

The majority of participants also agreed that the Annex A form was a step forward in terms of simplifying formalities, improving quality, and reducing translation costs.

In relation to the issuing of an EIO, the possibility of a proportionality check by the issuing authority was positively assessed, as was the consultation mechanism that can be triggered by the executing authority when it has reasons to believe that the proportionality requirement has not been met. The need for a secure communication network allowing EIOs to be safely transmitted was emphasized. Eurojust, the EJN, and the European Commission offered support, including work on the e-evidence platform to allow secure transmission of the EIOs and MLA requests.

At the time the meeting took place, no experience had yet been gathered regarding the application of grounds for non-recognition.

The time limits offered under the EIO regime were seen as an improvement compared to traditional MLA. However, regret was expressed that the Annex B form to acknowledge receipt is not often used in practice.

With regard to the application of the speciality rule, it remains unclear whether the EIO has changed anything in this regard or not. (CR)

Law Enforcement Cooperation

Further Concerns of EP Against E-Evidence Legislative Proposal

spot light

The EP rapporteur in the LIBE committee responsible for the Commission proposal on law enforcement access to e-evidence, *Birgit Sippel* (S&D, Germany), voiced further criticism (see already eucrim 4/2018, 206). After a first working document (see ibid.), *Sippel* and co-rapporteurs/shadow rapporteurs examined the following issues in several subsequent working documents:

- The scope of the application and the relation of the proposed instrument to other European instruments;
- The role of service providers;
- Relationship with third-country law, in particular the U.S. CLOUD Act;
- Conditions for issuing European Production Orders and European Preservation Orders and Certificates (EPOC(-PR)s);
- Safeguards and remedies;
- Enforcement of EPOC(-PR)s.

➤ *1. Scope of application and the relation of the proposed instrument to other European instruments*

In part A of the so-called "2nd working document" of 6 February 2019, *Sippel* and co-rapporteur *Nuno Melo* (EPP, Portugal) doubt whether the envisaged regulation on European Production and Preservation Orders for electronic evidence in criminal matters can be based on Art. 82 TFEU since it is not an instrument of mutual recognition which involves direct cooperation between judicial authorities, but concerns the execution of law enforcement orders by private providers. Furthermore, the EP rapporteurs stressed that it "needs to be made unequivocally clear" whether a Regulation is the right instrument or whether not a Directive is appropriate for an e-evidence legal framework.

Part B of the 2nd working document concludes that as regards subscriber data – "the data category required the most in trans-border cases, and needing swift action in order to start a criminal investigation and identify a suspect or link a suspect with a certain communication" – both the European Investigation Order and the CoE Cybercrime Convention represent a "forthcoming framework" despite their limitations.

➤ *2. Role of service providers*

In the third working document of 13 February 2019 (part A), Sippel and co-rapporteur *Daniel Dalton* (ECR, UK) question, *inter alia*, whether a fully-fledged fundamental rights assessment can and should be outsourced to private service providers. In this context, they note:

"The question of the possibility of outsourcing, even privatising, state prerogatives and sovereignty, relates to core (constitutional) prerogatives of a state, such as the protection of the fundamental rights of its citizens by its national constitutional provisions/traditions and international instruments, as well as the protection against potentially unjustified encroachments of foreign authorities on its territory in the judicial/law enforcement field."

Therefore, the question is whether the judicial authority of the state of enforcement need to be stronger involved.

In addition (part B of the third working document), the EP rapporteurs request the establishment of a reimbursement regime for the service providers. Finally, service providers need full legal certainty when it comes to their obligations and liability; they should not be left in a legal limbo between law enforcement/judicial orders, data protection obligations and third country laws. *Sippel* and *Dalton* conclude that "the proposed Regulation, however, seems to unfortunately exacerbate the legal uncertainty for the service providers."

➤ *3. Relationship with third-country law, in particular the U.S. CLOUD Act*

In the fourth working document of 11 March 2019 (Part A), *Sippel* and co-author *Sophie in't Veld* (ALDE, Netherlands) analyse the effectiveness of obtaining relevant e-evidence data by means of existing instruments of judicial cooperation, in particular by the 2003 EU-US Mutual Legal Assistance Agreement. They conclude that the MLA scheme is working satisfactorily. Therefore, a new instrument on direct access to e-evidence seems questionable where subscriber, access, and transactional data are concerned (at least when the major US providers are involved). As regards content data, improvements in the MLA agreement could be realised. In addition, the EU-US MLA agreement leaves enough room for strengthening judicial cooperation. According to the working document (Part A) the problem is not

the legislative side, but the adequate outfitting of judicial authorities handling MLA requests with adequate financial, human, and technical resources.

Part B of the 4th working document provides an in-depth look into the contents of the U.S. CLOUD Act (see also *Daskal*, eucrim 4/2018, 220–225). Sippel and in't Veld conclude that an EU e-evidence instrument would imply several incompatibilities with the US act and ultimately lead to conflicts of law. They also oppose Commission plans to get a mandate for negotiations with the USA – on behalf of the EU – on an executive agreement within the framework of the CLOUD Act. In view of the pending e-evidence proposal, this seems, *inter alia*, premature, as a number of questions have not yet been sufficiently answered before entering into negotiations with the USA.

Many shortcomings were also found in relation to Arts. 15 and 16 of the proposed e-evidence Regulation (Part C of the 4th working document); these provisions introduce a review procedure for cases in which the service provider, requested to produce data based on an EPOC, is faced with conflicting obligations from third-country law (e.g., if the service provider has its main seat in the third country).

➤ *4. Conditions for issuing EPOC(-PR)s*

In Part A of the 5th working document (8 March 2019), Sippel and co-rapporteur *Cornelia Ernst* (GUE/NGL, Germany) critically remark that the proposed rules on the issuing authority, which also entitle prosecutors to issue EPOCs/EPOC-PRs in cases of subscriber and access data, do not fully take into account constitutional constraints in many EU Member States. The authors fear a race to the bottom, which is why the necessity of judicial authorisations must also be considered in view of access data.

In view of the offences justifying the issuance of EPOC(-PR)s, there are concerns (as already mentioned in previous working documents) over reducing the protective role of authorities in the executing state. The proposal is a fundamental shift away from the existing *acquis* in judicial cooperation. The rapporteurs advocate the introduction of a stronger notification system with the right of the executing state to check, e.g., whether immunities or privileges are affected or whether the measure would be admissible in a similar domestic case (as provided by the EIO). They also advocate the right to oppose an EPOC(-PR) (see also Part B of the 5th working document). The latter should at least be possible when fundamental rights obligations are at stake. A double criminality test should take place if an EPOC refers to transactional and content data.

As further outlined in Part C of the 5th working document, *Sippel* and *Ernst* also voice concern over the total exclusion of the executing authority from being involved in proportionality checks. This also represents a paradigm shift from mutual recognition. It deprives the enforcement of coercive measures of the necessary checks and balances. Since the proportionality test seems the only safeguard against misuse, it might be advisable to think about more detailed and common rules on proportionality.

➤ *5. Safeguards and remedies*

Inconsistencies with existing mutual recognition instruments, e.g., the EIO, and the fact that the executing authority is kept out, also cause problems when it comes to notification of the data subject. In Part A of the 6th working document of 1 April 2019, *Sippel* and *Romeo Franz* (Greens/EFL, Germany) stress that EU legislation should introduce several parameters to resolve the tension between the interests of law enforcement authorities in withholding notifications and the data subject's interest in exercising his/her rights to defence and fair trial. It should be borne in mind that – according to the Commission proposal – it is only up to the issuing authority to inform.

In Part B of the 6th working document, *Sippel* and *Franz* examine the necessary *ex ante* safeguards, i.e., safeguards that must be guaranteed before e-evidence is collected and transferred to the issuing authority. The MEPs also found that *ex ante* safeguards necessitate stronger involvement of authorities in the executing state, including a comprehensive notification system and the possibility of a meaningful reaction to EPOC(-PR)s. Relevant rules could be modelled on Art. 31 and Art. 11 of the EIO Directive. A fundamental rights clause should be worded along the existing clause in the EIO Directive.

Such a notification mechanism triggers the question of which state must be notified. In order to guarantee efficient legal remedies, the "affected state" must be defined.

The effectiveness of remedies also plays a vital role for *ex post* safeguards. As further outlined in Part C of the 6th working document, Sippel and Franz question whether the data subject should have the right to not only challenge the legality of an EPOC in the issuing Member State, but also in the Member State of residence and/or the Member State of enforcement. Furthermore, the e-evidence proposal triggers the question of whether harmonised rules on legal remedies should be brought forward. The MEPs further note that the question of harmonisation is also raised for admissibility/exclusionary rules in the e-evidence context. The new EU tool must, however, at least specify which remedy applies if e-evidence has been obtained illegally.

In addition, *Sippel* and *Franz* identify further gaps in the Commission proposal, such as the prohibition of further processing and onward transfer of evidence, the inclusion of financial compensation and penalties for unlawfully acting issuing authorities, and remedies for service providers.

Ultimately, the MEPs fiercely reject the Commission's view (as mentioned in the impact assessment for the e-evidence proposal) that a "right to security" has to be balanced against other individual rights and safeguards. *Sippel* and *Franz* emphasise that such a position risks being below the level of the ECHR, where such a right

has not been legally recognised. It cannot be part of a balancing test.

➤ *6. Enforcement of EPOC(-PR)s*

In the 7th working document of 1 April 2019, Sippel and *Ignazio Corrao* (EFDD Group, Italy) deal with several aspects of the enforcement of EPOC(-PR)s in the Commission e-evidence proposal. They first disagree with the Commission's approach on leaving sanctions against providers for non-compliance with their obligations up to the national laws of the Member States. They advocate "some sort of harmonisation of the sanctioning regime." One reason is the risk of "forum shopping," since service providers may appoint their legal representative in the Member State with the lowest sanctioning regime.

Another critical issue is the proposed deadlines within which service providers must enforce EPOCs (in principle, 10 days upon receipt; in "emergency cases," 6 hours). The first challenge is that the deadlines might be too short for service providers to assess the legitimacy of an EPOC. Second, small- and medium-sized companies (SMEs) may not be able to meet the deadlines since they do not run 24/7 services. The same is true for third-country service providers that operate in different time zones. Third, the deadlines are not realistic for guaranteeing fundamental rights protection (if it is shifted to private companies). Therefore, the proposed deadline system must be reconsidered, either by introducing two separate deadlines (one for big companies, another for SMEs) or by setting up longer deadlines.

The 7th working document ultimately notes that the objection mechanism for service providers triggers many legal questions. Many concerns were voiced in previous working documents, e.g., regarding the involvement of the executing State authorities, the scope of the refusal grounds, and the level of information necessary for the service provider to make a meaningful legality check.

In this context, Sippel and Corrao conclude: "All these options are closely connected with the more general debate about mutual recognition in EU criminal law. The viewpoints on this issue vary substantially across Member States, national authorities, the Commission, CJEU, EC[t]HR, scholars and practitioners, and it becomes clear that the principle of mutual recognition is still under construction, closely connected to the changing nature of EU integration."

In sum, the working documents of the MEPs address several critical issues already voiced by European bodies and non-governmental organisations (see details at eucrim 4/2018, 206; 3/2018, 162–163, and 2/2018, 107–108). After these considerations, the EP blocked further negotiations with the Council before the Parliamentary Elections in May 2019. The hot debate over whether the e-evidence proposal is necessary and, if yes, which content it should have will be resumed with the newly composed EP in autumn. (TW)

Council Takes Position on Role of Legal Representatives in E-Evidence Cases

The European Parliament signalled that it is not eager to enter into trilogue negotiations on the proposed European Production and Preservation Orders for electronic evidence in criminal matters before the end of the parliamentary term in May 2019. The Council, however, went ahead with the second piece of the possible future legal framework on e-evidence, i.e., the proposed Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM(2018) 226 final, see eucrim 1/2018, 35–36).

The Ministers of Justice adopted a general approach on the Directive at the JHA Council meeting on 8 March 2019. The Directive will complement the Regulation by making it mandatory for service providers to designate a legal representative to receive, comply with, and enforce judicial orders on gathering e-evidence on the service providers' platforms. This is particularly relevant for service providers with headquarter in non-EU countries.

The general approach of the Council mainly changes the Commission proposal as follows:

- Extension of the applicability of the Directive, which should not only encompass electronic communications service providers, but also domain name registrars and related privacy and proxy services, in addition to "other information society providers that offer their users the ability to communicate with each other or offer their users services that can be used to process or store data on their behalf;"
- Legal representatives may not only be involved in gathering e-evidence, but also for orders based on other instruments of Title V, Chapter 4 TFEU, such as the Directive on the European Investigation Order or the 2000 EU Mutual Legal Assistance Convention;
- The designated legal representative under the Directive could be used for domestic procedures as well;
- Service providers and legal representatives should be held jointly and severally liable for non-compliance with their obligations deriving from the relevant legal framework on evidence;
- The obligations of service providers have been extended to make them responsible for providing the necessary resources and powers to guarantee compliance with orders and national decisions;
- The Council follows the Commission proposal as regards the Member States' obligation to establish effective, proportionate, and dissuasive sanctions against service providers if they do not comply with their duties; it has been clarified, however, that the financial capacity of the service provider must be taken into account when determining the sanction. This should especially reduce the burden for small- and medium-sized business entities (SMEs);
- Other specific arrangements for SMEs have been included, for instance the possibility to "share" a legal representative;

■ A full list of legal representatives shall be made publicly available to ensure easy access for law enforcement authorities (primarily but not only) via the European Judicial Network on criminal matters.

The European Parliament did not assess the proposal on the Directive before the end of the parliamentary term. It is anticipated that negotiations on the e-evidence legislative framework will be resumed after the new European Parliament takes up its work in autumn 2019. (TW)

Commission Wants Mandate to Negotiate International Rules on E-Evidence

On 5 February 2019, the Commission presented two recommendations to the Council that would allow the Commission to negotiate international rules for obtaining electronic evidence. The first recommendation relates to a possible "executive agreement" with the U.S. in the framework of the US CLOUD Act (see eucrim 4/2018, 207). The second recommendation aims at enabling the Commission to participate in negotiations on a second additional protocol to the Budapest Cybercrime Convention of the Council of Europe. The second additional protocol is currently discussed within the Council of Europe and intends to further strengthen this international cooperation including on obtaining access to electronic evidence, enhancing mutual legal assistance and setting up joint investigations.

It is now up to the Council to adopt the negotiating mandates. A first consideration on the ministerial level took place at the JHA Council meeting on 7–8 March 2019. The Romanian Council Presidency intends to have the adoption of the mandates until the end of June 2019 at the latest. (TW)

EDPS Gives Advice on Commission Mandate for EU-US E-Evidence Agreement

On 2 April 2019, the European Data Protection Supervisor (EDPS) issued an opinion on the Commission's plans to obtain a mandate from the Council to enter into negotiations with the USA over an agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters. The proposals were tabled by the Commission on 5 February 2019, and a first debate at the ministerial level took place from 7–8 March in the JHA Council.

The EDPS aims at delivering constructive and objective advice on the Council directives that will guide the Commission on several data protection issues in the negotiations.

The EDPS reminded the Commission and the Council that a future EU-US agreement on e-evidence should be based on strong safeguards for the individual's fundamental rights. The negotiating directive of the Council should include reference to the EU's data protection provision in Art. 16 TFEU. The agreement should also build on the EDPS recommendations on strengthened safeguards, which has been proposed in view of the EU-US Umbrella Agreement in 2016 (Opinion 1/2016).

In keeping with the proportionality principle, the EDPS specifically recommends that judicial authorities designated by the other party to the agreement be involved in the process of gathering electronic evidence as early as possible. This ensures that judicial authorities can effectively review the compliance of any requests for evidence with fundamental rights and raise grounds for refusal if appropriate.

The EDPS opinion also looks specifically into other aspects of the directive up for negotiation, such as the mandatory nature of the agreement, onward transfers, rights of the data subject, control by an independent authority, judicial redress, and administrative remedies, etc. (TW)

CCBE Makes Recommendations on Future E-Evidence Scheme

On 28 February 2019, the Council of Bars and Law Societies in Europe (CCBE) eyed recent developments at the EU and international levels to establish legal frameworks for cross-border access of law enforcement authorities to electronic evidence. The CCBE made several recommendations (available in English and French), which should be taken into account by the European institutions if they go ahead with the envisaged e-evidence legislation in the months to come.

The CCBE calls up the Commission and the Council to do the following:

■ Postpone negotiation of the proposed EU-US agreement and the Second Additional Protocol to the Council of Europe Convention on Cybercrime until the legislative process concerning the EU Regulation on European Production and Preservation Orders for electronic evidence in criminal matters is finalised.

■ Create sufficient safeguards and legal remedies, in particular against third-country surveillance measures;

■ Ensure the protection of client-lawyer communication;

■ Restrict the legal framework of direct cooperation with service providers in other jurisdictions to preservation orders only, thus enabling a meaningful legality check by the judicial authorities where the e-evidence is situated. The production of e-evidence should be followed up with a procedure under a Mutual Legal Assistance Treaty.

The CCBE statement, *inter alia*, lists several shortcomings of a direct cooperation scheme according to which service providers (as a private undertaking) can be compelled to comply with law enforcement orders from foreign states. Improvements in the current MLA schemes should be the preferred option. In the event that the European institutions decide to proceed with an e-evidence instrument based on direct cooperation, the CCBE makes several recommendations on minimum standards for such an instrument.

The new CCBE statement of 28 February 2019 comes after a first critical opinion of October 2018 on the Commission proposal for a Regulation on

European Production and Preservation Orders for e-evidence in criminal matters (see eucrim 3/2018, 162–163). The CCBE also voiced concerns over the planned cooperation between the EU and the USA within the framework of the U.S. CLOUD Act. In addition to several critical remarks in the above-mentioned statement, an in-depth analysis of the U.S. CLOUD Act is provided in an additional paper that was also issued by the CCBE on 28 February 2019.

CCBE Assesses U.S. CLOUD Act

The Council of Bars and Law Societies in Europe (CCBE) scrutinised the U.S. CLOUD Act. It allows U.S. federal law enforcement to compel U.S.-based technology companies to provide requested data stored on servers via warrant or subpoena − regardless of whether the data are stored in the USA or on foreign soil. By means of "executive agreements," it also foresees that law enforcement authorities from foreign "qualified countries" will have equal access to the data of U.S. companies (see eucrim 1/2018, p. 36, and the article by *J. Daskal* in eucrim 4/2018, pp. 220–225).

In a paper issued on 28 February 2019, the CCBE remarked positively that the CLOUD Act provides for a greater degree of legal certainty. Several concerns remain, however, in particular as regards its consistency with European law. The following issues are, *inter alia*, of general concern:

- Extraterritorial jurisdiction;
- Conflicts with the EU's fundamental rights and the GDPR;
- Weak (judicial) review;
- Lack of post-authorisation supervision;

The CCBE also voiced specific concerns over the lack of protection of legal professional privilege and professional secrecy. The current approach of the CLOUD Act deprives European citizens of this important European right, and disclosures would run contrary to several domestic laws of EU Member States.

In addition, the CCBE identified a gap in the existing U.S.-EU data protection scheme, since the Privacy Shield does not cover the transatlantic transfer from a private entity to government authorities for law enforcement and prosecution purposes.

In conclusion, the CCBE recommends that the EU negotiate a mutual legal assistance (MLA) treaty with the United States that explicitly refers to the U.S. CLOUD Act. Such an MLA treaty would provide precise requirements for the transfer of data and would not undermine the level of protection provided by fundamental freedoms valid in the EU.

Furthermore, a notification scheme should be established by means of which an independent European authority would be informed prior to a data transfer from a private entity to U.S. agencies.

On the basis of such an MLA treaty, legal professional privilege and professional secrecy must be an accepted ground for refusing data transfers to the USA under the CLOUD Act.

Together with the opinion of the EDPS of 2 April 2019 on negotiations planned between the European Commission and the USA over how to handle the transfer of e-evidence between the EU and the USA under the CLOUD Act (see eucrim 4/2018, 207), the CCBE paper is the second important contribution to the discussion on the "external dimension" of future international rules on e-evidence. Both the EDPS and the CCBE have come to similar, critical conclusions. (TW)

NGO Sees Lack of Key Safeguards in Planned E-Evidence Legislation

The plans to establish new rules that enable law enforcement authorities to directly seek the preservation and production of electronically stored data held by private service providers (the "e-evidence proposals", see eucrim 1/2018, 35–36) face further criticism from civil stakeholders. In February 2019, Fair Trials – a global watchdog that focuses on improving the right to a fair trial in accordance with international standards – issued a "Consultation Paper." It looks into the fundamental rights implications of the potential new legislation on e-evidence.

Fair Trials observes that the USA, with its CLOUD Act, and the EU, with the Commission proposal of April 2018 currently under negotiation, are about to set up a global "gold standard" as regards the effective cross-border access of law enforcement to electronic data. So far, however, human rights protections have only been vaguely recognised. Therefore, the consultation paper focuses on the following four key safeguards, which must be incorporated into the new mechanism:

- Prior notification of the suspect;
- Robust prior judicial authorisation procedure;
- Meaningful remedies in the event of a trial;
- Effective and systemic oversight on the use of the measures by law enforcement authorities.

Fair Trials concludes that the new EU rules on e-evidence, the U.S. CLOUD Act and the planned EU-US agreement on the exchange of e-evidence in criminal matters (see eucrim 4/2018, 207), can only serve as a global model if they "set high standards and uphold the fairness of criminal proceedings through real and meaningful safeguards." It further remarks: "In the absence of such safeguards, the new cross-border cooperation mechanism is likely to fail, causing injustice to the persons concerned and undermining public trust in law enforcement authorities."

The consultation paper, together with a more comprehensive "policy brief" released in October 2018, analysed the impact of current mechanisms for cross-border access to electronic data. The fairness of criminal proceedings was also taken into account in the critical working papers on the e-evidence proposal for a regulation on European preservation and production orders by the European Parliament's LIBE Committee. (TW)

Council of Europe*

Reported by Dr. András Csúri

Foundations

Human Rights Issues

Annual Activity Report by Human Rights Commissioner

On 8 April 2019, the Commissioner for Human Rights, *Dunja Mijatović*, presented her first annual activity report before the Parliamentary Assembly. Since taking up her work in 2018, the Commissioner visited several countries as an important means of dialogue, including Albania, Armenia, Estonia, and Greece. She paid particular attention to the following:

- Human rights in conjunction with immigrants, refugees, and asylum seekers;
- Media freedom and the safety of journalists;
- Children's and women's rights;
- Human rights protection in conjunction with counter-terrorism legislation.

As regards migration, the Commissioner calls upon Member States to improve the treatment of immigrants, respect human rights, and share responsibility in this matter. A particular issue of concern is the situation of individuals and NGOs who provide assistance to migrants, asylum seekers, and refugees, as increasing pressure and restrictions are being put on their work.

The report stresses the need for better protection of human rights advocates and journalists, as violent assaults, laws, and practices (e.g., against the right to confidential sources) significantly hinder their activities.

As regards women's rights, the report emphasises the need to tackle gender stereotypes and reduce the gender pay gap, which remain a major obstacle to achieving effective equality in both the public and private sectors. Additionally, violence against women must be efficiently investigated and prosecuted. The Commissioner also promoted the ratification and full implementation of the Istanbul Convention.

As regards children's rights, the Commissioner highlighted challenges connected to child poverty and equal access to quality-inclusive education for all children. The report identifies violence against children, including sexual abuse and exploitation of children, as another major issue. The Commissioner called on countries that have not yet done so to ratify both the Istanbul Convention, which protects children against domestic violence, and the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse. In this regard, the Commissioner also raised issues pertaining to juvenile justice, including the need to ensure that children have access to free legal aid and the importance of having a sufficiently high minimum age of criminal responsibility.

As regards the relationship between counter-terrorism measures and human rights protection, the Commissioner stressed that the misuse of anti-terrorism legislation has become one of the most common threats to freedom of expression, including media freedom. The report highlights that anti-terrorism legislation is typically adopted following accelerated procedures and/or in the direct aftermath of terrorist attacks, leaving little space for thorough and peaceful discussions on their human rights impact and thereby increasing the risk of misuse.

The report further summarized the Commissioner's activities against inequality faced by persons with disabilities, older persons, Roma, and LGBTI individuals.

Specific Areas of Crime

Corruption

GRECO: Fifth Round Evaluation Report on Malta

On 3 April 2019, GRECO published its fifth round evaluation report on Malta. The focus of this evaluation round is on preventing corruption and promoting integrity in central governments (top executive functions) and law enforcement agencies. The evaluation focuses particularly on issues, such as conflicts of interest, the declaration of assets, and accountability mechanisms (for more recent reports, see eucrim 1/2018, pp. 38–39; 2/2018, pp. 109–110 and 4/2018, p. 208).

GRECO notes that Malta has impressive anti-corruption mechanisms on paper, but these appear to be less effective in practice, especially when one looks at the controversies over the integrity of senior government officials in relation to the use of state resources and privatisation, tendering, land sales, or the award of contracts and public offices. So far, there has been no visible disciplinary or criminal response to any of these allegations.

The report highlights the lack of an overall strategy or a coherent risk-based approach when it comes to integrity

* If not stated otherwise, the news reported in the following sections cover the period 1 January – 31 May 2019.

standards and sanctions. GRECO calls for stricter rules and their enforcement in ancillary business and top officials' activities, conflicts of interest, and declarations of assets.

The report also calls for reforms to improve the capacity of the criminal justice system to respond to allegations involving senior officials. Certain institutions still have not achieved concrete results after 30 years of operation.

GRECO welcomes the appointment of a Chief Executive Officer in 2017 to modernise human resources management in the Maltese police force. The report recommends advisable improvements, including updated ethical standards, a performance-based approach to career decisions and promotions, and a stronger training system. The Independent Police Complaints Board must be strengthened, including safeguards for informants.

GRECO: Fifth Round Evaluation Report on The Netherlands

On 22 February 2019, GRECO published its fifth round evaluation report on The Netherlands, which calls upon the Dutch authorities to further intensify corruption prevention measures, both in top executive functions and vis-à-vis members of law enforcement agencies.

GRECO notes that the integrity of the country's government is based mainly on political accountability. This needs to be complemented by a clear integrity strategy vis-à-vis managers − based on risk analysis −, however, to better avoid conflicts of interest and thus potential corruption.

GRECO recommends establishing a code of conduct for top executives/officials, including measures for its implementation and enforcement as well as introducing rules for lobbying and post-employment functions. Top executives should be required to report conflicts of interest on an *ad hoc* basis and to declare personal assets at regular intervals.

As regards police authorities, the report recognises a strong commitment towards integrity and a high level of public trust. Nevertheless, there have been breaches of integrity, e.g., information leaks and links to organised criminal groups.

Lastly, GRECO recommends improving the existing codes of conduct for both law enforcement authorities and training systems, with particular attention to ensuring the use of confidential information and the declaration of financial interests by officials holding particularly sensitive posts. In addition, officials should report all forms of corruption-related misconduct within the service, not only those classified as criminal offences.

GRECO: Fifth Round Evaluation Report on Poland

On 28 January 2019, GRECO published its fifth round evaluation report on Poland. The report recognizes the progress made, including the new anti-corruption programme for 2018–2020 and the improved transparency of interaction with lobbyists. However, GRECO raises serious concerns and, as a top priority, recommends addressing the establishment of an objective and transparent system for the appointment, promotion, and dismissal of senior managers in the Police and Border Guard as well as addressing the corruption risks arising from the current system of asset declaration.

Concerning law enforcement agencies, the report highlights that three Chief Commanders have headed the Police in the space of just two years. In addition, low salaries make it more difficult to find qualified staff and lead officials to take up part-time jobs, leading to incompatibilities and problematic relations with third parties.

With regard to the risk of corruption among "persons entrusted with top executive functions" (PTEFs) in the central government, the report expresses concern over the lack of clear rules and guidelines for gifts. International opinion polls show that a large number of Poles regard corruption as widespread and that business representatives see too close a link between politics and business.

As regards the asset declaration system, the report welcomes the declaratory obligations for assets and interests of PTEFs, including those co-owned with spouses, but notes that the picture may be blurred if changes are made to the regulation of matrimonial property. Additionally, systematic awareness-raising activities are missing for PTEFs.

GRECO describes the verification of asset declarations by Poland's Central Anti-Corruption Bureau (CAB) as inadequate, due to the general nature of the data, which merely refers to the number of declarations received. In addition, GRECO raises concerns about the independence of CAB, as it is under the authority of the Prime Minister and of a designated "minister-coordinator for special services." Therefore, GRECO recommends establishing an independent review mechanism with adequate means to perform its tasks in an effective and accountable manner.

GRECO: Belarus Non-Compliant with CoE Anti-Corruption Standards

In an unprecedented move on 19 March 2019, GRECO publicly proclaimed in a Declaration that Belarus does not comply with the anti-corruption standards of the CoE.

Of the 24 recommendations that GRECO had addressed to Belarus in 2012, twenty were not followed and the rest were only at a "generally unsatisfactory" level of conformity. The majority of the recommendations concerned basic anti-corruption requirements, such as strengthening the independence of the judiciary, increasing the operational autonomy of law enforcement, and limiting immunity protection. In addition, Belarus has never authorised the publication of any evaluation or compliance reports by GRECO.

Such continued non-compliance calls into question both the commitment and cooperation of Belarus as such in the

fight against corruption. *Marin Mrčela*, President of GRECO, stressed that these recommendations are not only elements of an effective fight against corruption, but are also the core principles of GRECO and the CoE.

GRECO urged all its 49 Member States to disseminate the Declaration within their administrative and financial institutions and also warned them to take this situation into account in their future contacts with Belarus. In the meantime, GRECO continues to monitor the situation.

Money Laundering

MONEYVAL: Fifth Round Evaluation Report on the Czech Republic

On 11 February 2019, MONEYVAL published its fifth round evaluation report on the Czech Republic. The fifth evaluation round builds on previous MONEYVAL assessments by strengthening the examination of how effectively Member States prevent and combat ML and terrorism financing (TF). For background information, see eucrim 1/2018, pp. 40–41; 2/2018, p. 111, and 3/2018, pp. 208–210 for further references.

The report acknowledges the accuracy of the risk assessments by Czech authorities. Correspondingly, ML occurs mostly in conjunction with tax crimes, fraud, corruption, phishing, and subvention fraud. The probability of FT occurring remains low. That said, MONEYVAL calls for more explicit analysis.

Although banks have an appropriate understanding of ML/FT risks, the awareness is lower at other financial institutions.

MONEYVAL acknowledges the legislative reforms and progress made in pursuing ML investigations. The report casts doubt, however, on the efficiency of the existing supervisory model in a view of limited resources. Though some large-scale ML cases led to convictions, the report recommends pursuing more investigative opportunities with regard to serious third party and stand-alone ML. The prevalent practice within the Czech justice system of sanctioning multiple offences simultaneously makes it difficult to measure the precise impact of a sentence solely related to ML.

The report emphasizes improvements within the legislative and institutional framework on seizure and confiscation. Financial investigations resulted in significant amounts being seized and confiscated. Additionally, financial investigations carried out in relation to terrorism offences also brought to light the possibility of FT activities occurring in the Czech Republic. In response, law enforcement managed to plausibly identify the respective roles of suspects in FT-related schemes.

The Commercial Register in the Czech Republic is accessible directly and free of charge, but the quality and accuracy of the information varies.

In conclusion, the report praises the Czech authorities for their active cooperation with foreign colleagues. This is also demonstrated by the fact that, in addition to mutual legal assistance, other forms of international cooperation are routinely used both spontaneously and upon request.

MONEYVAL: Fifth Round Evaluation Report on Lithuania

On 8 February 2019, MONEYVAL published its fifth round evaluation report on Lithuania. As regards national risk assessment, Lithuania faces a number of ML threats, mainly from corruption, the shadow economy, organised crime, and the widespread use of cash. Concrete results are apparent in reducing the shadow economy, but further efforts are needed, especially in the investigation and prosecution of ML and AML/CFT supervision.

There is no information available on increased FT risk in Lithuania. MONEYVAL reports that the Lithuanian authorities have a disparate, but largely appropriate understanding of this issue, which matches the country's risk profile.

The authorities have presented a number of ongoing cases of complex ML, where convictions are still pending. Most of the ML convictions obtained to date relate to self-laundering. A more uniform and effective approach within law enforcement is needed, for example, to identify the level of evidence required to convince the judiciary that the means originate from criminal activity, even in the absence of a criminal conviction. Sanctions have the potential to have a deterrent effect, but have not yet been used to full effect.

The confiscation of proceeds from crime is a priority objective. The identification of proceeds from crime has improved, and the volume of assets seized provisionally has increased significantly. Nevertheless, the volume of assets seized remained modest.

As regards FT, there were only two reported cases in Lithuania. While control mechanisms exist, the skills necessary to deal with such cases still need to be developed. In addition, the report recommends that Customs Service be given further powers to stop/restrain currency at borders in order to determine whether evidence of ML/FT can be found. MONEYVAL states that Lithuania exhibits characteristics of an effective system of targeted financial sanctions (TFS), where financial institutions are aware of designations by the UN and EU and have customer and transaction screening systems. However, the legal framework for TFS is not fully in line with FATF Standards. There is no formal procedure in place to identify targets of designations, no designation has been made or proposed, and no funds have been frozen under the TFS regime.

Lastly, MONEYVAL acknowledges that Lithuania has a sound legal and procedural framework for exchanging information with foreign partners. The country actively seeks international cooperation with other states, which has led to convictions and the seizure and confiscation of proceeds of crime.

Articles

Articles / Aufsätze

Fil Rouge

Following impetus from the Treaty of Lisbon, the EU became increasingly active in procedural aspects of criminal law, particularly in the sphere of gathering evidence and access to evidence. The core instrument for gathering evidence located in another EU Member State – the European Investigation Order (EIAO) – is now in full use. However, legal and practical challenges were aired at a meeting of legal practitioners at Eurojust in September 2018. *J. Guerra* and *C. Janssens* recapitulate the main findings of this meeting. They also give an overview of the major problems to be solved by practitioners in the near future when the EIO is applied – if necessary with Eurojust's support. *J. Espina Ramos* tackles the EIO's relationship with other judicial cooperation instruments – an important and practical problem. Since the Directive leaves questions open as to the applicability of other instruments next to or instead of the EIO, he develops three rules to guide legal practitioners in applying the correct legal instrument.

A. Soo and *A. Pivaty* address the defendant's right to access case materials during the pre-trial stage. They focus on unclear aspects of Art. 7 of Directive 2012/13, especially its derogations from the right of (unlimited) access to the case materials in para. 4. National judges are encouraged to raise questions on interpretation of the provision before the CJEU, so that this important right for the defendant is further defined at the EU level.

A. Juszczak and *E. Sason* envision future prospects of Union-wide evidence gathering by asking whether it is advisable to extend the European Public Prosecutor Office's competence to investigations of terrorist offences. They present the pros and cons of a Commission proposal and conclude that an alternative way forward could be a more targeted approach, e.g., to gradually extend the EPPO's competences, starting with areas distinctly linked with PIF crimes.

Thomas Wahl, Managing Editor of eucrim

Legal and Practical Challenges in the Application of the European Investigation Order

Summary of the Eurojust Meeting of 19–20 September 2018

José Eduardo Guerra and Christine Janssens

After implementation of Directive 2014/41 by the EU Member States (bound by the Directive) in 2017 and the first half of 2018, the European Investigation Order (EIO) has become the core instrument for obtaining evidence located in another EU Member State. The EIO simplifies and accelerates cross-border investigations, but practical and legal challenges remain. Such challenges as well as first experiences and best practices in the application of the EIO were discussed among practitioners at a meeting organised by Eurojust in September 2018. This article summarises the main results of the meeting.

Participants acknowledged the need to interpret national law in light of EU law, in line with the principles of mutual recognition and mutual trust, but also underlined the challenge of constantly searching for legally sound and practically feasible solutions between different national legal systems. They agreed on the importance of an overall pragmatic and flexible approach. Views diverged on several topics (e.g. the speciality rule, costs in the context of the proportionality test), but coincided on many others. Recommendations relate *inter alia* to the scope of the EIO, the use of the forms, the language regime and time limits. Participants envisaged that the support of Eurojust in relation to EIOs will probably be higher, when compared to the MLA regime, as more consultations are foreseen in the EIO Directive. Whilst participants acknowledged that "direct contact" amongst judicial authorities is the core principle of the Directive, they strongly believed that, in bilateral cases, Eurojust's bridge-making role can facilitate communication between the judicial authorities involved if one of the consultation procedures is triggered and that, moreover, in complex multilateral cases Eurojust has a unique and important coordinating role.

I. Introduction

On 19–20 September 2018, Eurojust organised a meeting on the Directive regarding the European Investigation Order in criminal matters (hereinafter EIO DIR).[1] Practitioners from the EU Member States as well as representatives from EU institutions and academia met at Eurojust in plenary sessions and workshops. The meeting provided a forum for practitioners to identify several practical and legal challenges in the application of the EIO, to exchange experience and best practice and to discuss how Eurojust and the European Judicial Network (EJN) can further support the national authorities. This article recapitulates the outcome report[2] and addresses the following main issues that were brought forward during the meeting:

- Scope of the EIO;
- Competent authorities;
- Content, form, and language of the EIO;
- Issuance and transmission of an EIO;
- Recognition and execution of an EIO;
- Specific investigative measures;
- Possible support provided by EU actors.

II. Scope of the EIO Directive and Its Relation to Other Legal Instruments

The fact of having one stand-alone legal instrument covering all types of investigative measures (with the exception of Joint Investigation Teams , or JITs) in the field of evidence gathering within the EU was welcomed and considered as a major step forward. That being said, several questions were raised as to whether a specific measure falls within the scope of the EIO DIR or not and whether the use of another legal instrument should take precedence.

According to Art. 34(1) EIO DIR, the EIO replaces only the corresponding provisions of the conventional MLA instruments. The term "corresponding provisions" remains a point of concern. In the absence of a common EU list,[3] it has become clear that in relation to some measures and provisions different interpretations exist in the Member States, which sometimes leads to frictions. Participants mentioned cases where judicial authorities were reluctant to execute a measure requested/ordered under the wrong legal instrument, but in general terms it can be said that judicial authorities have been pragmatic and have executed an EIO *as if it were* an MLA request or have executed an MLA request *as if it were* an EIO. Participants expressed the need for further guidance on the meaning of the term "corresponding provisions" and reflected together on which guiding criteria could be helpful in assessing whether an EIO needs to be issued (or not) in relation to an on-going investigation in the issuing Member State.[4] Participants agreed that the following criteria could be helpful in assessing whether the EIO DIR should apply:

- the order concerns an investigative measure aimed at gathering or using evidence,
- the measure was issued or validated by a judicial authority, and
- the measure relates to Member States bound by the EIO DIR.

If one of these requirements does not apply, the EIO DIR would not be the right instrument to use and another legal instrument would need to be applied. For instance, if a measure has no "evidence" related implications, but a mere procedural objective (e.g. service and sending of procedural documents), an MLA request, and not an EIO, should be sent.

In some cases, EIOs have been issued for several types of measures with different aims, for instance, an EIO for a house search *and* for the delivery of a document. Most participants agreed that, in cases where the delivery of a document is instrumental to the investigative measure that is the object of the EIO, its inclusion in the EIO would be in line with the EIO DIR. If, however, the delivery of the document is not instrumental, different views exist to the effect that in some Member States judicial authorities will execute the EIO while in other Member States judicial authorities will insist on receiving an additional MLA request.

Another problem is posed in relation to freezing measures, where the EIO DIR replaces Framework Decision 2003/577/JHA only as regards evidence gathering, but not as regards subsequent confiscation (Art. 34(2) EIO DIR). While participants agreed that it is for the issuing authority to make this assessment and to clarify the purpose of the freezing measure, there have been cases where executing authorities questioned the assessment made by the issuing authority and refused to execute the measure under the EIO DIR and demanded a freezing certificate instead of the EIO.

On the subject of the gathering of evidence in real time (Art. 28 EIO DIR), most participants believed that the wording of this provision is sufficiently broad as to leave room for measures such as video/audio surveillance, tracking or tracing with the use of technical devices (GPS) and accessing a computer system. However, no consensus was reached regarding the possibility of applying Arts. 30 and 31 EIO DIR, i.e. the provisions on the interception of telecommunications, in cases of tracking devices ("bugging of a car").

The wording of recital 25 of the EIO DIR which sets out that the EIO can be applied "at all stages of criminal proceedings" and which delineates the EIO from the European Arrest Warrant (EAW) in case of temporary transfer of persons, also triggered discussion. First, participants discussed whether an EIO can be used beyond the trial phase. In general, participants believed that such use would be limited to Member States where the notion of criminal proceedings includes the execution phase and provided that Framework Decision 2008/947/JHA[5] would not apply in the concrete case. Secondly, participants discussed the possibility of using an EIO instead of an EAW for the transfer of persons in cases where the thresholds of Framework Decision 2002/584/JHA[6] are not met. Their views on this matter were divided, but most participants considered that the EIO DIR offers the appropriate legal basis for the transfer of persons whenever the person concerned must give evidence during an investigation or before a court, irrespective of whether the thresholds of the Framework Decision on the EAW are met. If the EIO DIR is applied, some participants emphasised, however, that, since this measure concerns a deprivation of liberty, a judge in the issuing Member State should be involved, at least in the practical arrangements under Art. 22(5) EIO DIR.

III. Competent Authorities

The enhanced role for judicial authorities in the issuing phase of the EIO, and particularly the requirement that, when an EIO has not been issued by an (investigative) judge, a court or a public prosecutor, it needs to be validated by one of these authorities before its transmission (Art. 2(c)(ii) EIO DIR), was perceived to be a positive evolution of the system, serving to enhance mutual trust as the driving force of the principle of mutual recognition. Furthermore, participants from Member States where this need for a validation by a judicial authority has been introduced as a novelty in their national legal system explained that it has improved cooperation between law enforcement and judicial authorities and entailed the latter's earlier involvement in the investigations.

The issue whether the executing authority can carry out preliminary checks on the judicial nature of the issuing/validating authority was considered, by most participants, to be in line with Art. 9(3) EIO DIR.

As regards competent authorities in the executing phase, participants also concluded that a specialised receiving authority that acts as a single point of contact can be beneficial for various reasons. First, it can internally improve efficiency by avoiding duplication or overlaps of incoming EIOs. Second, it can ensure a unified response vis-à-vis the issuing authority, particularly in cases where several local prosecutors or investigating courts are involved in the execution of the EIOs.

IV. Content, Form and Language of the EIO

A majority of participants welcomed the form to be used for EIOs (Annex A of the EIO DIR) and saw it as a step forward in terms of simplifying formalities, improving quality and reducing costs of translation. Some concrete suggestions for best practices for the filling in of the form were made, *inter alia*:

- Including the name of the suspect(s) even though the measure does not apply to him/her to avoid potential *ne bis in idem* situations;
- Highlighting the requested measures;
- Listing the questions to be addressed to a witness/victim/suspect.

As to the use of section D of the form in Annex A of the EIO DIR, participants acknowledged the narrow wording of the segment "relation to an earlier EIO", but favoured a broader interpretation whereby this box would also be used to provide relevant information on related past or future judicial cooperation requests such as upcoming EIOs or other mutual recognition orders, mutual legal assistance requests, or JITs, including existing JITs with other States in the framework of multilateral coordination settings.

The advantages and/or disadvantages of sending one EIO or multiple EIOs were also addressed, particularly in complex

cases where different measures are required concerning different natural and legal persons with a different procedural status. In such cases, the internal coherence and consistency between the different sections of the form in Annex A, in particular between sections C, D, E, G, H and I, is a shared concern. For this reason, some practitioners prefer to issue several EIOs instead of one stand-alone EIO. Participants also argued that, for reasons of confidentiality, it may also be advisable, in some cases, to issue separate EIOs rather than just one, depending on the legal regimes in the Member States concerned and/or the stage of proceedings in the Member States involved. It was suggested that Eurojust assistance may be useful to decide on the best approach in the case at hand and to ensure continuity in the executing phase.

When asked whether minor changes to the content of an EIO would require the issuing of a new EIO, different views were expressed. Some authorities require a new EIO while others take a more flexible approach. Participants believed that this would primarily depend on the type of correction needed. For instance, if the correction relates to a new address, this would probably require a new EIO. However, it was also noted by some participants that, in urgent cases, the formal part of issuing a new EIO could be done at a later stage, after the execution of the measure.

In some cases, either the issuing authority submits, or the executing authority requests, additional documents, e.g. the national judicial decision underlying the EIO. Some participants wondered whether any parallels could be drawn with the *Bob Dogi* judgment,[7] particularly if coercive measures are at stake. Most participants considered that neither the EIO DIR nor their national legislation requests the domestic order to be attached to the EIO. Some emphasised that a reference to the domestic order in the EIO with full details of that order should be sufficient. Other participants added that, unlike Art. 8(1)(c) EAW FD, Art. 5(1) EIO DIR does not impose any legal requirement for the domestic judicial decision to be mentioned or attached to the EIO. A minority of participants noted that, under their national law, the attachment of a domestic order is required. In that case, pragmatic solutions are identified, e.g. the EIO is kept simple and the domestic order (more lengthy) is attached with or without translation. Participants from Member States where the attachment of the domestic order is not required also acknowledged that, depending on the case, the attachment of the national court order may be useful, for informative purposes, for instance in cases where a coercive measure is requested and the executing Member State is also required to issue a court order.

In relation to the language regime (Art. 5(2) EIO DIR), it was held that, in general, it does not create many problems. In case of urgent requests, the practice among Member States varies: some require a translation into their official language while others allow a second language to be used for the EIO. Participants also underlined the importance of accepting one common, widespread language.

V. Issuance and Transmission of an EIO

In relation to the issuing of an EIO, participants discussed the proportionality check by the issuing authority as foreseen in Art. 6(1) EIO DIR. Discussions also addressed the consultation mechanism that can be triggered by the executing authority when the latter has reasons to believe that the proportionality requirement has not been met (Art. 6(3) EIO DIR). Participants assessed this consultation mechanism positively and argued that it can be used to provide relevant information and to avoid the risk that the execution is refused. Participants also believed that Eurojust is in a privileged position to contribute by serving as a bridge-maker between both, the issuing and executing authorities.

The relevance of costs and whether cost-related issues should be taken into consideration for the proportionality check were matters of debate. Whilst there was a consensual approach that cases involving costs "deemed exceptionally high" can be resolved through the consultation mechanism included in Art. 21(2) EIO DIR, participants held different views in relation to cases involving costs that are *in se* not exceptionally high, but that relate to minor offences and, if repeated, could entail high costs. Some participants explained that, in their Member States, executing authorities are receiving a huge amount of EIOs related to small offences and are struggling to cope with all these requests. Some participants underlined that a *de minimis* criterion cannot be used as a *de facto* ground for non-recognition. The grounds for non-recognition are exhaustively mentioned in the EIO DIR and constitute exceptions to the principle of mutual recognition, which should be interpreted restrictively. Other participants added that Member States which apply the mandatory prosecution principle, as opposed to the discretionary prosecution principle, would not be entitled to take cost-related criteria into consideration.

In relation to the transmission of an EIO (Art. 7 EIO DIR), participants indicated that the sending of the EIO directly to the executing authority or to the dedicated, specialised receiving authority, is the rule, but they also added that, depending on the nature, complexity and urgency of the case, different channels are being used, including Eurojust, EJN Contact Points or Liaison Magistrates. Participants underlined the importance of a secure network of communications allowing them to transmit EIOs in a safe manner.

VI. Recognition and Execution of an EIO

1. Grounds for non-recognition

Since the EIO is a relatively new instrument, experience in the application of the grounds for non-recognition (Art. 11 and Chapters IV and V of the EIO DIR) is still somehow limited. Participants mentioned other issues that can also complicate the execution of EIOs, even if they are not grounds for refusal, in particular: (i) lack of information; (ii) bad translations and (iii) different status of a person to be heard (witness in the issuing Member State and suspect in the executing Member State). It was underlined that in none of these cases a refusal is acceptable, but communication between the involved authorities should be established as soon as possible to find the appropriate solution. In relation to the three aforementioned scenarios, it was argued that Eurojust could provide useful support when direct contact between judicial authorities is hampered.

2. Recourse to another investigative measure

Participants mentioned several cases where the executing authorities had recourse to a different type of investigative measure (Art. 10 (1) EIO DIR). For instance, in some cases, executing authorities had recourse to production orders instead of house searches. In another case where the issuing authority had ordered a witness hearing with a view to obtaining banking information in the EIO, the executing authority had recourse to a house search instead of a witness hearing because house searches were the standard procedure in the executing Member State for these types of cases. When discussing these cases, participants concluded that the frequent use of Art. 10 (1) EIO DIR highlights the challenges created by the different legal systems in the Member States, particularly the different legal prerequisites for investigative measures. Whilst in many cases the differences are relatively easily overcome and solutions are found as a result of the consultation procedure and the direct contact between the competent authorities involved, there have also been other cases where the consultation procedure and the direct contact threatened to come to a standstill. Participants suggested that in particularly complex, sensitive and/or urgent cases, Eurojust can play a vital role.

3. Time limits

Participants welcomed that the EIO DIR provides for a form that acknowledges the receipt of an EIO (Annex B of the EIO DIR), but deplored that in practice the form is often not used. They underlined the importance of using this form and held that, if the time limits of Art. 12 EIO DIR cannot be met, the executing authority should explain the reasons for the delay to the issuing authority and the latter should be immediately informed of a feasible time frame. Participants agreed that, under no circumstances should the delay be a cause or reason for non-execution.

4. Urgent requests

Participants noted that most Member States tend to adopt a pragmatic and flexible approach in relation to urgent cases. From their experience, the execution of urgent EIOs can start on the basis of mutual trust and formal requirements are fulfilled later on. For instance, practitioners mentioned cases where the execution of EIOs started even though the translation was not yet available at the time of the execution, but was provided later on. Participants underlined, in this regard, the importance of accepting the use of one common/widespread language in order to facilitate the execution of urgent requests. In relation to urgent cases, participants also agreed that a timely involvement and intervention of Eurojust can be crucial.

5. Speciality rule

Participants were divided in relation to the application of the speciality rule in the context of the EIO DIR, i.e. to what extent evidence gathered by means of this instrument can be used by the issuing State in other investigations or shared with other Member States or third countries. Some participants affirmed the application by relying on Art. 19(3) EIO DIR (on confidentiality), but a large majority of participants believed that this provision is not at all related to the speciality rule and underlined that there is no explicit provision in the EIO DIR which addresses this issue. Some participants held that the EIO DIR has not changed anything in relation to the speciality rule and argued that this rule still applies under the new regime. Others believed that, under the EIO regime, the issuing authority becomes the owner of the evidence and is entitled, subject to national and EU data protection rules, to transfer it further, unless the executing authority has prohibited such transfer explicitly. As a result of these different views, participants follow different approaches when issuing or executing EIOs. From the executing Member State's perspective, some participants indicated that they explicitly mention, when executing an EIO, that the evidence can only be used for the purpose of that specific investigation, often fearing that it might be used in another case without this explicit wording. Others stated that they would not specify anything, but would assume that the evidence will not be used for another purpose. From the issuing Member State's perspective, some participants indicated that, before using the evidence in a different case, they would always ask permission from the executing Member State. Oth-

ers considered that a request for permission to use the evidence for another purpose is not required since it is a matter for the issuing authority to decide upon, subject to the applicable legal framework on data protection.

VII. Specific Investigative Measures

1. Hearing by videoconference

The EIO DIR sets out rules on specific investigative measures. Art. 24 EIO DIR provides for the possibility to hear witnesses or experts or even suspects/accused persons by videoconference or other audio-visual transmission. Art. 24(2) EIO DIR sets out additional grounds for non-recognition beyond those of Art. 11 EIO DIR. Participants first discussed to what extent the absence of the suspected or accused person's consent constitutes a mandatory or optional ground for non-recognition. The implementation in the national laws of the EU Member States is diverse. Some only allow the hearing of a suspected or accused person by videoconference if the person consents ("*shall*" refuse, mandatory ground for non-recognition) whilst others are less rigid ("*may*" refuse, optional ground for non-recognition). Some participants suggested that in cases where grounds for non-recognition are being raised, the legal systems of both the issuing and executing Member States should be given close consideration and the assistance of Eurojust could be helpful.

Participants also discussed whether a hearing by videoconference could be allowed to guarantee the participation of a defendant in his criminal trial. It is not common practice and in most Member States' national legislation on such hearing by videoconference is not foreseen. Some participants firmly stated that the execution of an EIO directed to a videoconference replacing the defendant's presence at trial would therefore not be allowed under their national law. Other participants stated that their national law does not regulate it, but noted that – since it is not explicitly prohibited and it is considered not contrary to the fundamental principles of the executing Member State's law – EIOs have been executed, provided that the defendant's rights were guaranteed.

2. Interception of telecommunications without technical assistance

Regarding the specific provisions of the Directive on the interception of telecommunications, a point of discussion was particularly the interception of telecommunications with no technical assistance needed from the Member State where the subject of the interception is located (Art. 31 EIO DIR), which obliges the intercepting Member State to notify the Member State on whose territory the subject of the interception is or will be ("the notified Member State"). Participants heavily debated to what extent a notified authority can check whether "*the interception would not be authorised in a similar domestic case*" (Art. 31(3) EIO DIR). While most participants agreed that this should be a merely formal, procedural check, several participants indicated that in some Member States it is a substantive examination whereby additional information is requested to make the assessment. This often leads to decisions imposing a termination of the interception (if it is still ongoing) and/or a prohibition to use the intercepted material. Most participants rejected a detailed, substantive approach and argued that it is not in line with the *ratio legis* of Art. 31 EIO DIR. The purpose of the notification is *not* an order for recognizing an investigative measure (Annex A), but a mere reflection of respect for the sovereignty of the other country. It would be a paradox if in the context of the relevant Annex C form the same or more information would be requested than in the frame of an Annex A form. Participants believed that the provision should be interpreted in the light of the values of the area of freedom, security and justice, based on mutual trust and respect for different legal systems. Against this background, most participants believed that Article 31(3) EIO DIR should not be interpreted in an extensive way. Participants also discussed the consequences of a lack of notification and/or a lack of approval. They expressed concerns with regard to the admissibility of the evidence. Some participants stated that the evidence obtained would not be considered admissible. Other participants noted that in cases where the lack of notification was due to the authorities not knowing where the person was, it had not led to the inadmissibility of the evidence.

VIII. Support Provided by EU Actors

Eurojust explained how it can support practitioners in the four crucial phases of the life cycle of an EIO: the (pre)issuing phase, the transmission phase, the recognition phase and the execution phase, both in bilateral and multilateral cases. In bilateral cases, Eurojust can provide support, for instance, in:

- Identifying the competent authority;
- Completing (draft) EIOs;
- Clarifying legal and practical issues in relation to other legal instruments;
- Obtaining/providing necessary additional information in the context of one of the consultation procedures that the EIO DIR foresees (e.g. in relation to the proportionality check, the recourse to a different type of investigative measure or the application of a ground for non-recognition);
- Finding balanced solutions where different national systems clash.

In multilateral cases, Eurojust has a unique coordinating role, particularly in complex cases where action days are planned simultaneously in different Member States and where Eurojust can provide support in the context of a coordination meeting and/or a coordination centre.

The Secretary to the EJN informed the practitioners about the assistance the EJN Contact Points can provide in EIO cases and on the useful tools and information for the practical application of the EIO DIR available on the EJN website.[8] The website provides direct access to the Compendium, a tool that enables an EIO to be drafted online and saved as a work file at any time. Other relevant tools are the Judicial Atlas (which can be used to identify the locally competent authority that can receive the EIO), the fiches belges (which contain concise and practical legal information on what is possible in the respective Member States) and the Judicial Library (which includes, *inter alia*, the full text of the EIO DIR and the word forms of the three Annexes).

The European Commission underlined that smooth cross-border gathering of evidence requires that Member States have the EIO DIR properly implemented in their national laws and correctly applied in practice. There are special tools in place for assessing national laws/practice and for, where necessary, improving knowledge among practitioners (e.g. expert meetings, awareness building projects, training). In relation to the secure transmission of EIOs and MLA requests, the Commission underlined that the work on the e-evidence platform is currently ongoing and is expected to be finalized by the end of 2019. The Commission also confirmed its commitment to drafting a Handbook on the EIO, but noted that it may take several years to finalize it since it is important that the Handbook integrate practical information from the Member States and relevant case law.

IX. Conclusions

From a general perspective, a vast majority of the participants at the 2018 Eurojust meeting on the European Investigation Order very much welcomed the new regime and see the instrument, with its characteristic mutual recognition features – e.g. standard form, judicial authorities in charge, limited grounds for refusal and time limits – as a step forward in the area of cross-border evidence gathering. Only a small number of participants perceived the new instrument, and particularly its template, as more complicated and more cumbersome than before.

During the meeting, participants discussed a number of suggestions and/or best practices in relation to a variety of topics, including the scope of the EIO DIR (e.g. cumulative criteria to assess whether an EIO should be issued), the competent authorities (e.g. the EJN Judicial Atlas for the identification of the competent authorities), the EIO forms in Annexes A, B, C of the EIO DIR (e.g. how to fill in certain sections), the language regime (e.g. the acceptance of one common, widespread language) and time limits (e.g. duly informing the issuing authority of the reasons for a delay and suggesting an alternative feasible time frame). In relation to some other topics, participants held different or even opposing views (e.g. the proportionality test, particularly in relation to the issue of costs and the applicability of the speciality rule).

A majority of participants agreed that the differences that exist within the area of freedom, security and justice in the EU are challenging and require an overall pragmatic and flexible approach towards the legal systems of other Member States. "Direct contact" amongst judicial authorities is the guiding principle of the EIO DIR, yet in complex, sensitive or urgent cases Eurojust's unique coordinating and bridge-making role can be crucial. It can facilitate communication between the judicial authorities involved and Eurojust's expertise, professional distance from the cases concerned and mediating role can bring added value for finding a balanced and legally sound solution.

José Eduardo Guerra
Deputy to the National Member for Portugal and Vice-Chair of the Judicial Cooperation Instruments Team at Eurojust

Christine Janssens
Judicial Cooperation Advisor at the Operations Department and member of the Judicial Cooperation Instruments Team at Eurojust

*This text is a recapitulation of the Outcome Report of the Eurojust Meeting on the European Investigation Order, organised by Eurojust in The Hague on 19–20 September 2018 (see endnote 2).

1 Directive (EU) 2014/41 regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.

2 Eurojust, "Eurojust meeting on the European investigation order, The Hague, 19–20 September 2018, *Outcome Report*", Council document 15735/18. The report is also available at: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategicmeetings/Outcome%20report%20of%20the%20Eurojust%20meeting%20on%20the%20European%20investigation%20order%20(19-20%20September%202018)/2018-12_Outcome-Report_Eurojust-meeting-on-EIO-Sept2018_EN.pdf. See

also *eucrim*. See also *Riehle*, https://eucrim.eu/news/eurojust-meeting-report-european-investigation-order/.

3 Apart from Council doc. 14445, there is not (yet) a detailed list available indicating exactly which provisions will be replaced. In 2017, Eurojust and EJN issued a Joint Note, Council doc. 9936/17, which gathers *inter alia* the views of the EJN contact points on the question of which measures they consider would be excluded from the scope of the EIO DIR.

4 See also the article of Jorge A. Espina Ramos, "The European Investigation Order and Its Relationship with Other Judicial Cooperation Instruments", in this issue.

5 Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions, *O.J. L 337, 16.12.2008, 102.*

6 Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States, *O.J.* L 190, 18.7.2002, 1.

7 ECJ, 1 June 2016, Case C-241/15, *Bob Dogi*. In this judgment, the CJEU decided that, in light of Art. 8(1)(c) Framework Decision 2002/584/JHA, a EAW cannot be issued directly, but requires a prior national arrest warrant. For the purpose of Art. 8(1)(c) FD EAW, the expression "arrest warrant" means a national warrant that is distinct from the EAW and on which the latter is based.

8 https://www.ejn-crimjust.europa.eu/ejn/EJN_StaticPage.aspx?Bread=10001.

The European Investigation Order and Its Relationship with Other Judicial Cooperation Instruments

Establishing Rules on the Scope and Possibilities of Application

Jorge A. Espina Ramos

"Evolution is a change from an indefinite, incoherent homogeneity, to a definite coherent heterogeneity".

Herbert Spencer (First Principles, 1862)

I. Introductory Remarks

The Directive regarding the European Investigation Order,[1] is fully applicable in practice now that 26 EU Member States, which are bound by the new instrument of judicial cooperation, have completed the transposition process.[2] It is a significant step forward in judicial cooperation when it comes to the trans-border gathering of evidence. The EU legal framework has been aligned with the provisions of Art. 82 TFEU, which indicates that "judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions (…)."

However, the European Investigation Order (hereinafter: EIO) is not the only applicable instrument for the purpose of trans-border gathering of evidence within the EU. Not all EU Member States are bound by the EIO Directive.[3] In fact, under certain circumstances, the Directive does not preclude the application of other international conventions on mutual legal assistance (MLA) by judicial authorities. Therefore, practitioners need a clear idea as to the situations in which it is compulsory to use an EIO, when it would be merely convenient to use it, or when it would be impossible to gather evidence abroad by means of an EIO.

Against this background, this article analyses the Directive and establishes a number of rules that clarify the scope and possibilities of application of the new instrument. These rules will help legal practitioners to decide whether an EIO is possible or not in any given case. They also offer guidance on the question of which provisions have been replaced by the EIO Directive and when certain conventions retain their applicability for trans-border evidence-gathering purposes. The rules will be categorised as follows:[4]

- A *Basic Rule* that defines the elements necessary for the issuing of an EIO (II. below);
- A *Replacement Rule* (III. below) that regulates the substitution of the following:
  – Certain parts of traditional MLA conventions and protocols that governed the gathering of evidence abroad between the EU Member States before the EIO;[5]
  – Two specific instruments of mutual recognition, i.e. Framework Decision 2008/978/JHA on the European Evidence Warrant (hereinafter: FD EEW), which was fully replaced by the EIO, and Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence (hereinafter: FD Freezing) that was only partly replaced by the EIO (as regards provisions connected with freezing of evidence).

- A *Complementarity Rule* that enables judicial authorities to continue to use other conventions for evidence-gathering purposes, provided that certain conditions are met (cf. below IV.).

II. The Basic Rule

As a starting point, it is necessary to analyse when the EU legislator wants the EIO to be used, because this will avoid misunderstandings in practice and ensure that the correct instrument of judicial cooperation is chosen in each individual case. We should therefore look at the following general provisions of the Directive, which indicate parameters on the applicability of the EIO:

> Art. 1(1): "A European Investigation Order (EIO) is a judicial decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') to have one or several specific investigative measure(s) carried out in another Member State ('the executing State') to obtain evidence in accordance with this Directive. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State".
>
> Art. 3: "The EIO shall cover any investigative measure with the exception of the setting up of a joint investigation team and the gathering of evidence within such a team (…)".

These provisions on the aim and scope of the Directive must be read together with Art. 34(1), which does not provide for all provisions of the traditional MLA conventions and protocols to be replaced by the EIO but only the "corresponding provisions" (see further the Replacement Rule below III.). An accurate definition of the scope of the EIO by means of a Basic Rule is a precondition for clarification of which provisions of traditional MLA conventions and protocols can no longer be applied.

Instead of simply listing the provisions to be replaced by the EIO, the proposed approach is a guiding norm. From this norm it can be established when an EIO is necessary and, vice versa, when, due to lack of some of the elements of this Basic Rule, an EIO is not possible. First, this approach should be followed, because the legislator expressly decided not to include a legal list in the Directive, which would indeed have solved many uncertainties and led to legal certainty.[6] Second, attempts (by Eurojust and the EJN in a Joint Note,[7] as well as by some national authorities[8]) to set up a list including the various provisions from traditional MLA conventions and protocols deemed to still be valid resulted in an excessively casuistic approach. Such lists – no matter how comprehensive they are – risk opening the door to new examples and interpretations, thus even undermining the much needed legal certainty.

Taking the norms concerning the scope and aim of the EIO as the foundation of the Basic Rule, the rule can be formulated as follows:

"The EIO is
1) a decision issued (or validated) by a judicial authority; within criminal proceedings (in the sense defined in Art. 4 of the Directive);
2) consisting in investigative measures of trans-border nature;
3) aimed at gathering evidence;
4) among the Member States bound by the EIO Directive.
When conditions set out in numbers 2 to 5 concur, the judicial authority must issue an EIO, unless other instruments are better placed to produce the desired results provided the conditions in the Compatibility Rule under Art. 34(3) of the Directive are met.
Conversely, if any of the five conditions above is missing, an EIO cannot be issued."

The new system based on the EIO is to be considered the preferred option whenever the necessary conditions are met, and this is reflected in recital 35.[9] It can also be seen to be a consequence of the general principle already quoted in Article 82.1 TFEU above, placing criminal judicial cooperation under the umbrella of the mutual recognition principle.

However, the applicability of this Basic Rule is subject to two caveats. In other words, there are two specific situations[10] in which the EIO cannot be used, even though all criteria of the Basic Rule are met:

- Evidence gathered within Joint Investigations Teams (hereinafter: JITs), because Art. 3 of the EIO Directive declares the continuation of the regulation on JITs as provided under Art. 13 of the 2000 MLA Convention and in Council Framework Decision 2002/465/JHA.
- Evidence-gathering rules provided by former or future EU mutual recognition instruments that must be considered *lex specialis* (e.g., requests for criminal records[11] or the gathering of e-evidence under a possible future Regulation[12]).

III. The Replacement Rule

The Basic Rule must be supplemented by a Replacement Rule. The latter takes up the provision in Art. 34 of the EIO Directive, which reads as follows:

> "1. Without prejudice to their application between Member States and third States and their temporary application by virtue of Article 35, this Directive replaces, as from 22 May 2017, the corresponding provisions of the following conventions applicable between the Member States bound by this Directive:
>
> (a) European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959, as well as its two additional protocols, and the bilateral agreements concluded pursuant to Article 26 thereof;
>
> (b) Convention implementing the Schengen Agreement;
>
> (c) Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol.

> 2. Framework Decision 2008/978/JHA is hereby replaced for the Member States bound by this Directive. Provisions of Framework Decision 2003/577/JHA are replaced for Member States bound by this Directive as regards freezing of evidence.
>
> For the Member States bound by this Directive, references to Framework Decision 2008/978/JHA and, as regards freezing of evidence, to Framework Decision 2003/577/JHA, shall be construed as references to this Directive."

Art. 34(1) clarifies that the EIO prevails over traditional MLA conventions and protocols that were the main legal basis for evidence-gathering in the context of judicial cooperation in criminal matters. The EIO is now the instrument to be used for such purposes, as the corresponding provisions of said conventions have been replaced.

Art. 34(2) establishes a similar rule, but it addresses two specific evidence-related instruments of mutual recognition, the FD EEW and the FD Freezing. Both instruments overlap with the scope of the new EIO Directive. Whereas the FD EEW has been fully replaced, the FD Freezing has only been partially replaced, i.e., as regards its provisions on the freezing of evidence (see also above).

On this basis, a Replacement Rule could be formulated as follows:
"Evidence-gathering provisions (the "corresponding provisions") from the traditional MLA conventions and protocols, the entire FD EEW, and provisions concerning freezing of evidence under FD 577/2003/JHA, are replaced by the EIO Directive and cannot be used, provided the Basic Rule applies."

The connection with the Basic Rule is necessary insofar as the replaced provisions are not to be used when an EIO is applicable.[13]

1. Replacement vs. repeal

Emphasis must be placed on the fact that the Directive is *replacing* but not *repealing* the traditional MLA conventions and protocols and the two specific mutual recognition instruments, respectively.[14] There are three main reasons for this approach:

- Formal reasons: The Directive cannot repeal the traditional MLA conventions and Protocols (even if that had been its intention), because specific formal rules exist for repealing or withdrawing from international treaties. The same holds true for repealing EU instruments, e.g., the FDEEW (see also below).
- Territorial reasons: The EIO is not a binding instrument for all EU Member States. Therefore, the traditional MLA conventions and protocols must remain in place in order to continue cooperation with Denmark and Ireland as well as with third countries that are parties to these international treaties.
- Substantive reasons: As mentioned above, the replacement is limited to the "corresponding provisions" connected to the gathering (or to the freezing) of evidence, i.e., the EIO Directive takes only a sectorial approach.

It should be noted, however, that, despite the provision in Art. 34(2) of the EIO Directive, the FD EEW was repealed by Regulation 2016/95 of 20 January 2016.[15] Although this led to the FD EEW being fully expelled from the EU legal framework, the EIO Directive did not foresee this consequence. The repeal was made two years after publication of the EIO Directive and by means of a specific repeal instrument; thus, it did not stem from Art. 34(2). The legislator of the EIO Directive initially did not want to permanently eliminate the EEW from the legal scenario.

2. Examples of non-replaced provisions

As a complement to the system of the Basic Rule and as clarification for the Replacement Rule, the following text passages offer several examples of specific provisions that can be considered not to have been replaced by the EIO Directive. The various cases, in which certain provisions from the traditional MLA conventions and protocols appear to remain applicable, have been systematised in three categories. As we will see, the Basic Rule as discussed above (II.) serves as the basis for the findings below.

a) Non-replaced provisions due to the policing (and non-judicial) nature of the cooperation

First, cooperation can have a non-judicial nature. This affects, for instance, trans-border surveillance (provided for in Art. 40 CISA), which is even specifically mentioned as not being a covered measure – and therefore not being replaced by recital 9 of the Directive. Another example is hot pursuit (provided for in Art. 41 CISA).

Both measures are also specifically mentioned in the Joint Note Eurojust-EJN, and there seems to be wide consensus among practitioners that the EIO does not replace them. In my view, this is true, as long as they are considered police measures.

It can also happen that a judicial authority decides to carry out trans-border surveillance.[16] In the affirmative, this would not be a police but a judicial measure and must therefore be vetted in accordance with the criteria of the Basic Rule. It follows that such cases would require an EIO: the provision of Art. 40 CISA would not be applicable, because it is not a measure of police cooperation but a judicial one.[17]

In addition, the Joint Note Eurojust-EJN includes the provisions of Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence, the measures mentioned in Art. 39(2) CISA, and the measures under the Naples II Convention (customs cooperation) as not being replaced by the EIO. In contrast to the Joint Note, which mentions these provisions/measures in the context of the corresponding provisions not replaced by Art. 34(1) of the Directive, it must be borne in mind that these are different instruments – they are therefore *per se* not subject to the Replacement Rule of the Directive.

b) Non-replaced provisions because there is no evidence-gathering purpose

Widespread consensus has been reached that certain measures, which are not specifically aimed at gathering evidence – and therefore do not meet the corresponding criteria of the Basic Rule, can be considered excluded from the scope of the EIO. As a result, traditional rogatory letters (hereinafter: LoRs) or mutual legal assistance requests must be used for such activities in accordance with the traditional conventions and protocols. This comprises, for instance, service of documents and summons (Art. 5 of the 2000 MLA Convention), the spontaneous exchange of information (Art. 7 of the 2000 MLA Convention), returning objects to the injured party (Art. 8 of the 2000 MLA Convention), and transfer of proceedings or information with a view to proceedings being opened by another country (Art. 21 of the 1959 MLA Convention).[18] The EIO never intended to cover these cases (cf. Art. 1 and 3 of the Directive).Although this matter has not been the subject of in-depth discussions yet, judicial requests aimed at taking down an Internet server should be added to this category of measures, which pursues a different goal than evidence-gathering. Such requests are becoming increasingly common in cases of cybercrime and cyberattacks, where this measure is necessary − not so much to gather evidence but to ensure that the criminal activity is discontinued. It is therefore a sort of precautionary measure but not an evidence-gathering one. Thus, it also does not meet the Basic Rule but would instead require a traditional LoR.[19]

c) Non-replaced provisions by virtue of law

As indicated under II., Art. 3 of the EIO Directive specifically provides for the continuation of previous JIT provisions under the 2000 MLA Convention and the so-called JIT Framework Decision. This is a logical exclusion from the EIO scope, because the very nature of a JIT allows evidence-gathering measures to be taken internally, and the evidence gathered is automatically put at the disposal of all parties to the JIT without the need to resort to other judicial cooperation instruments. Therefore, the JIT legal framework excludes LoRs, which is why it makes sense to maintain the same regime in the EIO context that (only) replaces most traditional LoRs.

Without prejudice to the express provision of Art. 3, in my view, the exclusion of JITs can also be deduced from the Basic Rule: the trans-border nature of the measures adopted as part of a JIT does not in practice mean that any of the judicial authorities involved actually issue orders to be executed beyond its jurisdiction. Quite the opposite is true: measures are discussed and agreed following an operational plan for each specific case as provided for in the JIT Agreement; each judicial authority issues orders and executes measures exclusively within its own jurisdiction. As a result, judicial decisions lack the trans-border element of the Basic Rule, which is why an EIO would not have been possible anyway. In sum, the exclusion of JITs from the scope of the EIO may be considered more natural than apparent at first sight. The rationale of Art. 3 is, on the one hand, to legally establish the remaining validity of Art. 13 of the 2000 MLA Convention (and thus clarify that it is not part of the replaced "corresponding provisions") and, on the other, to protect the normal functioning of a JIT, precluding the use of EIOs as long as the JIT is operational.

IV. The Compatibility Rule

Whereas Art. 34(1) of the EIO Directive posits the EIO as the heir to traditional Conventions and Protocols, Art. 34 (3) and (4) open the way for the applicability of other cooperation instruments if the purpose of the EIO can be better achieved by them. The wording of the relevant paragraphs of Art. 34 is as follows:

> "3. In addition to this Directive, Member States may conclude or continue to apply bilateral or multilateral agreements or arrangements with other Member States after 22 May 2017 only insofar as these make it possible to further strengthen the aims of this Directive and contribute to simplifying or further facilitating the procedures for gathering evidence and provided that the level of safeguards set out in this Directive is respected
>
> 4. Member States shall notify to the Commission by 22 May 2017 the existing agreements and arrangements referred to in paragraph 3 which they wish to continue to apply. Member States shall also notify the Commission within three months of the signing of any new agreement or arrangement referred to in paragraph 3."

Art. 34(3) indicates that other cooperation instruments can be applied only under certain conditions, which can be traced back to the default situation, as stated in Art. 82 TFEU, that judicial cooperation must be based on the mutual recognition principle. As a result, we can formulate a Compatibility Rule as follows:

"Even in cases where the Basic Rule would apply, existing or future bilateral or multilateral agreements or arrangements (but not the traditional MLA conventions and protocols replaced under Article 34(1)) could be used instead of the EIO,

if the alternative instrument complies with all three of the following conditions:
a) further strengthens the aims of the EIO Directive,
b) simplifies or further facilitates the procedures for gathering evidence, and
c) respects the level of safeguards set out in the Directive.
Failing to comply with the obligation defined under Article 34(4) to notify to the Commission the above agreements does not affect applicability of the agreements/arrangements.
The Compatibility Rule does not apply to other (existing or future) EU mutual recognition instruments, which could be applicable instead of the EIO as lex specialis, but not due to the provisions of Art. 34(3).”

1. The conditions of the Compatibility Rule

The wording in the EIO Directive indicates that the three conditions indicated in the Compatibility Rule are not alternative but cumulative, i.e., all of them must concur so that an alternative instrument is possible. Thus, any other bilateral or multilateral instrument can be used instead of an EIO only inasmuch as it offers at least a similar standard on safeguards (condition c)) and provided that the use of this alternative instrument results in better, simpler, and faster cooperation (conditions a) and b)).

2. The scope of the Compatibility Rule

The Compatibility Rule refers to “*bilateral or multilateral agreements or arrangements with other Member States.*” This concept includes all sorts of international instruments (treaties and conventions) which the EU Members States concerned are parties to (even if it is a multilateral convention that also includes third countries, e.g., the conventions concluded in the framework of the Council of Europe or the United Nations). This opens the door for the applicability of a number of specific instruments (e.g., the 2001 Budapest Convention on Cybercrime) if the above-mentioned specified conditions are met.

By contrast, the wording of the Compatibility Rule entails that it cannot be applied to (existing or future) EU mutual recognition instruments– because they are not “*agreements or arrangements*”, but pieces of EU legislation. The provision of Art. 34(4) also underpins this argument because a notification to the Commission can logically not include pieces of EU legislation that are perfectly known to the Commission. As mentioned under II. other EU legislation on cross-border gathering of evidence can apply instead of an EIO as *lex specialis*, as it is e.g. the case for criminal records or – as far as future instruments are concerned – under the *lex posterior* rule (e.g. the European Preservation and Production Orders on e-evidence), but not as a consequence of the Compatibility Rule.

3. The relationship between the Compatibility and the Replacement Rule

There is much discussion among practitioners as to whether the Compatibility Rule can be applied also to provisions affected by the Replacement Rule.[20] In my opinion, Art. 34(1) of the Directive, i.e., the Replacement Rule, takes precedence over Art. 34(3), i.e., the Compatibility Rule. Consequently, a judicial authority is not able to use a LoR instead of an EIO, even if the use of a replaced provision on evidence-gathering in the traditional conventions and protocols would fulfil the conditions of the Compatibility Rule in a given case. The Replacement Rule is not conditional or optional, but a clear imperative legislative decision that allows for no exceptions.

This position is backed by the ECJ case law.[21] With regards to similar provision in Art. 31 of the Framework Decision on the European Arrest Warrant, the ECJ held in *Goicoechea*:[22]

> “Article 31(2) of the Framework Decision allows the Member States to continue to apply bilateral or multilateral agreements or arrangements in force at the time of adoption of the decision, or to conclude such bilateral or multilateral agreements or arrangements after the entry into force of the decision in so far as they allow the prescriptions of the decision to be extended or enlarged and help to simplify or facilitate further the procedures for surrender of persons who are the subject of European arrest warrants.
>
> However, that provision cannot refer to the conventions mentioned in Article 31(1) of the Framework Decision, since the objective of the decision is precisely to replace them by a simpler and more effective system (…).”

Albeit, the ECJ’s decision refers to a different cooperation instrument, i.e., the European Arrest Warrant. The parallelism to Art. 34 of the EIO Directive is obvious, and there are no reasons to sustain a different interpretation for the EIO in this respect.

4. Notification to the European Commission

Some clarifications need to be made as regards the notification of existing or future agreements/arrangements in accordance with Art. 34(4) of the EIO Directive. Questions have been raised as to the nature of this provision and as to whether the lack of notification would prevent an EU Member State from continuing to use such bilateral or multilateral conventions. In my opinion, the lack of notification should not affect the applicability of the conventions themselves. The first reason for this stance is that the notification is not included in Art. 34(3) as a further condition for application of the Compatibility Rule. The EU legislator conceived it as a separate Member State obligation. Accordingly, notifications are considered to be differ-

ent from a legal condition, instead intended to give clarity to the applicable legal framework. While the conditions set out under Art. 34(3) are addressed to individual judicial authorities (which assess the applicability of a different instrument instead of an EIO), Art. 34(4) addresses the Member States as such. With the regulation in two different paragraphs of Art. 34, it is thus made clear that the purpose and consequences of the two provisions are fundamentally different.

Secondly, a too rigid interpretation would lead to every Member State having to notify virtually any convention or treaty ever concluded in the area of international cooperation in criminal matters – and those concluded from this moment onwards – in order to avoid the risk of doubt as to the validity of the evidence gathered through other instruments.

Third, it would be contrary to the established international rules if the mere lack of communication to the Commission produces legal effects of validity, because international treaties follow their own formal rules (see also above III.1.).

V. Excursus: The Continuing Applicability of the Speciality Principle

During the discussions on the applicable rules, a specific question was raised as to whether the speciality principle continues to apply under the EIO. The speciality principle was originally developed in the area of extradition law and can be understood in the present context as precluding the issuing authorities from using the evidence received via the execution of an EIO for any other purposes and proceedings than those for which the EIO was originally issued, unless specifically authorised to do so by the executing authority. The issue on the continuation of the speciality principle under the EIO regime surely deserves more in-depth reflection, but in view of its high practical relevance, some brief comments on this problem are appropriate, especially since the question is also connected to the rules developed above.

The issue was discussed at the 2018 Eurojust Meeting on the EIO[23] without consensus being reached and the unclear situation was subsequently acknowledged at the level of the Council Working Group.[24] In my opinion, the speciality principle has not been affected by the EIO Directive and continues to be valid.[25]

A first reason relates to Art. 6 of the EIO Directive. It establishes that the issuing authority must assess the necessity and proportionality of the measures "for the purpose of the proceedings" and whether those measures "could have been ordered under the same conditions in a similar domestic case." These factors can also be controlled by the executing authority, triggering a consultation process. In my view, this implies the remaining validity of the speciality principle, because, otherwise, it would be absurd to establish a system based on the necessity and the proportionality check of measures linked to a concrete case if, after having received the results of the execution, the issuing authority remained free to use them for any other proceedings, thus rendering the safeguards provided for in Art. 6 completely useless.

Second, another element of the speciality principle is data protection rules, which stipulate the purpose limitation principle. However, this principle of data protection law is governed by Art. 23 of the 2000 MLA Convention 2000[26] – a provision that, in my opinion, has not been replaced by the EIO Directive. In this context, the Basic and Replacement Rules come into play: Art. 23 cannot be considered a replaced corresponding provision and therefore remains fully applicable and unaffected by the EIO Directive. The understanding that the purpose limitation principle has not been cast aside by the EIO is also mirrored by some transposition legislation, e.g., the Spanish Law on Mutual Recognition.[27] It also seems to be the position of the European lawmaker as regards the future Regulation on European Preservation and Production Orders.[28]

From a practical viewpoint, a third argument is, ultimately, that it hardly seems encouraging if executing authorities do not have assurance that information provided will not be used for other purposes or proceedings than those specifically stated in any given EIO.

VI. Conclusions

This article illustrated that the question on the relationship between the EIO and other – existing or future – legal instruments of judicial cooperation in criminal matters is currently one of the major challenges in practice. I strived to develop a theoretical blueprint from which decisions can be drawn in each concrete case. The developed rules include the necessary clarification for all legal practitioners as to when an EIO is to be used:

Basic Rule

(defining when an EIO is to be used):

"The EIO is
5) a decision issued (or validated) by a judicial authority;
6) within criminal proceedings (in the sense defined in Art. 4 of the Directive);
7) consisting in investigative measures of trans-border nature;
8) aimed at gathering evidence;
9) among the Member States bound by the EIO Directive.

When conditions set out in numbers 2 to 5 concur, the judicial authority must issue an EIO, unless other instruments are bet-

ter placed to produce the desired results provided the conditions in the Compatibility Rule under Art. 34(3) of the Directive are met.
Conversely, if any of the five conditions above is missing, an EIO cannot be issued."

Replacement Rule

(developed from Art. 34(1) and (2) of the EIO Directive, defining the exclusion of the applicability of other existing evidence-gathering provisions):

"Evidence-gathering provisions (the "corresponding provisions") from the traditional MLA conventions and protocols, the entire FD EEW, and provisions concerning freezing of evidence under FD 577/2003/JHA, are replaced by the EIO Directive and cannot be used, provided the Basic Rule applies."

Compatibility Rule

(stemming from Art. 34(3) and (4) of the EIO Directive, indicating the co-existence of the EIO with other judicial cooperation instruments):

"Even in cases where the Basic Rule would apply, existing or future bilateral or multilateral agreements or arrangements (but not the traditional MLA conventions and protocols replaced under Article 34(1)) could be used instead of the EIO, if the alternative instrument complies with all three of the following conditions:
a) further strengthening of the aims of the EIO Directive;
b) simplification or further facilitation of the procedures for gathering evidence;
c) respect for the level of safeguards set out in the Directive.
Failure to comply with the obligation defined under Article 34(4) to notify to the Commission of the above agreements does not affect applicability of the agreements/arrangements.
The Compatibility Rule does not apply to other (existing or future) EU mutual recognition instruments, which may be applicable instead of the EIO as lex specialis, but not due to the provisions of Art. 34(3)."

In addition to the above and as regards the speciality principle, it must be understood that it remains valid and applicable to the EIO Directive.

Jorge A. Espina Ramos
Spanish Desk of Eurojust

1 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *O.J.* L 130, 1.5.2014, 1.
2 The Directive had to be transposed by 22 May 2017. However, it took until 15 September 2018 for the last Member State to complete the transposition, finally making the Directive fully applicable in practice for all.
3 According to recitals 44 and 45 of the Directive, Ireland and Denmark are not bound by it, in accordance with Protocols No. 21 and 22 annexed to the TEU and the TFEU.
4 I first suggested this three-tiered approach based on "Basic, Replacement and Complementarity Rules" in my presentation on "*The EIO and its Relationship with other Conventions*" at the Summer Course organised by the Universidad Internacional Menéndez Pelayo in Santander on 20–22 August 2018. A similar approach as regards the Basic Rule was also mentioned in the Conclusions of the Eurojust Meeting on the EIO that took place on 19–20 September 2018 (cf. Council doc. 15735/18 and the article of Guerra/Janssens, in this issue).
5 According to Article 34.1, these are the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959 (hereinafter: 1959 MLA Convention), its two additional protocols, and the bilateral agreements concluded pursuant to Art. 26 thereof; the Convention implementing the Schengen Agreement (hereinafter: CISA); and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol (hereinafter: 2000 MLA Convention).
6 There was an attempt in 2011 to define a list of corresponding provisions to be replaced by the EIO (Council doc. 14445/11), but the effort was then abandoned and no further progress was made.
7 "Note on the meaning of corresponding provisions and the applicable legal regime in case of delayed transposition of the EIO Directive," 2 May 2017, Council doc. 9936/17. The Note contains interesting reflections on these topics.
8 A number of Member States have also tried to provide answers to some of the open questions either through provisions in the implementing legislation or through Instructions or Notes prepared by the relevant national authorities (regularly General Prosecution Offices). One example is Note 1/17 issued by the International Cooperation Unit of the Spanish General Prosecutor's Office of 19 May 2017, where consideration is given to which provisions of the traditional conventions and protocols could still be valid after entry into force of the EIO.
9 Recital 35 specifically declares: "Where reference is made to mutual assistance in relevant international instruments, such as in conventions concluded within the Council of Europe, it should be understood that between the Member States bound by this Directive it takes precedence over those conventions."
10 See also III.2.c) and IV.2 below.
11 Framework Decision 2009/316/JHA on the establishment of the European Criminal Record Information System (ECRIS).
12 See the proposal by the Commission for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final), currently being discussed in the European Parliament and Council. For details, see eucrim 4/2018, 206 with further references and *S. Tosca*, eucrim 4/2018, 212 et seq.
13 If, for whatever reasons, an EIO is not due, the "corresponding provisions" are applicable (because they have not been replaced). This would be the case, for instance, for requests concerning Denmark or Ireland.
14 In line with the Joint Note Eurojust-EJN, mention should be made of

a case-law precedent unequivocally supporting this distinction between replacing and repealing. It is connected to a different instrument, the European Arrest Warrant, where a similar situation arose (the EAW Framework Decision also used the mechanism of replacing existing extradition conventions) and where the European Court of Justice (case C-296/08) had the chance to rule that "the replacement under Article 31(1) of the Framework Decision of the conventions mentioned in that provision does not entail the abolition of those conventions, which retain their relevance (…) also in other situations in which the European arrest warrant system is not applicable."

15 *O.J.* L 26, 2.2.2016, 9–12.

16 This caveat would also be valid for hot pursuit measures under Art. 41 CISA, at least in theory. It appears much more difficult to find a realistic example where something as spontaneous and unpredictable as a hot pursuit could be decided beforehand by a judicial authority.

17 In addition: Art. 17 of the 2nd Additional Protocol to the 1959 Convention, which refers to *judicial* trans-border surveillance, does not apply either, because it is fully affected by the Replacement Rule and is among the provisions replaced by the EIO Directive.

18 See also the Joint Note Eurojust-EJN, *op. cit.* (n. 7).

19 Whether this measure should be based on the traditional MLA conventions and protocols or on a different legal instrument (in particular, the 2001 Budapest Convention on Cybercrime of the Council of Europe) is connected to the Compatibility Rule (see below) but not to the Replacement Rule.

20 See, in this context, particularly Germany's declaration of 14 March 2017, which indicated that bilateral agreements supplementing the 1959 MLA Convention are considered to continue to apply to cross-border acquisition of evidence.

21 See also Joint Note Eurojust EJN, *op. cit.* (n. 7), p. 23.

22 CJEU, 12 August 2008, case C-296/08 (*Ignacio Pedro Santesteban Goicoechea*), paras 54 and 55 (emphasis added by the author).

23 See note 4.

24 Council doc. 14750/18 of 27 November 2018.

25 See also J. Barbosa e Silva, "The Speciality rule in cross-border evidence gathering and in the EIO – let's clear the air", (2019) 19 *ERA Forum*, 485–504.

26 "Personal data communicated under this Convention may be used by the Member State to which they have been transferred: (a) for the purpose of proceedings to which this Convention applies; (b) for other judicial and administrative proceedings directly related to proceedings referred to under point (a); (c) for preventing an immediate and serious threat to public security; (d) for any other purpose, only with the prior consent of the communicating Member State, unless the Member State concerned has obtained the consent of the data subject."

27 Article 193 of Law 23/2014, as amended by Law 3/2018, copies the wording of Art. 23(1) of the 2000 MLA Convention stating that the Spanish issuing authority will guarantee use of the personal data obtained by way of execution of an EIO to be limited to the proceedings for which they were requested, or on those directly linked to them, requiring specific authorisation from the executing authority for all other cases.

28 Even though the proposal from the Commission did not contain a provision on the speciality principle, negotiations in the Council Working Group apparently ended up including a new article regulating such a speciality principle, roughly along the lines provided for by said Art. 23 of the 2000 MLA Convention. The instrument is still being discussed by the European Parliament, but the reaction at the Council level is an indication of what the opinion of the EU lawmakers might be on this issue.

Access to the Case Materials in Pre-Trial Stages

Critical Questions of Article 7 of Directive 2012/13/EU on the Right to Information in Criminal Proceedings

Anneli Soo, PhD and Anna Pivaty, PhD

The right of access to the case materials (Art. 7 of Directive 2012/13/EU) is crucial to enable an effective defence and ensure equality of arms in criminal proceedings. However, when it comes to the pre-trial stages of criminal proceedings, Art. 7 of Directive 2012/13/EU is not clear about the timing of access, the scope of access, and about the possible derogations from providing access to suspects and their counsel.

This article outlines the questions that, in our opinion, should most urgently be posed to the CJEU concerning the interpretation of Art. 7 in the context of pre-trial proceedings, e.g.: What are the documents that are "essential for challenging effectively" the lawfulness of arrest and detention under Art. 7(1)? Do the grounds for derogation under Art. 7(4) apply to Art. 7(1)? How should the derogation grounds under Art. 7(4) be understood? Do Art. 7(2) and (3) apply at the pre-trial stages of the proceedings, and particularly to pre-trial investigations? If yes, what is the scope and manner of access to the case materials that should be provided at these stages? We argue that further interpretation from the CJEU is necessary to ensure greater uniformity and stronger protection of the right of access to the case materials across the EU Member States.

I. Introduction: The Right of Early Access to the Case Materials in EU Law

In EU law the right of access to the case materials in criminal proceedings arises from Art. 7 of Directive 2012/13/EU on the right to information in criminal proceedings.[1] Two elements of the right are distinguished:

- The right of access upon arrest or detention (Art. 7(1));[2]
- General right to access the case materials (Art. 7(2) and (3)).[3]

- Art. 7(4) provides the grounds for derogation from the right.[4]

Directive 2012/13/EU was adopted on 22 May 2012 and had to be transposed by 2 June 2014. The CJEU has addressed interpretation of its Art. 7 only once so far.[5]

Art. 7 is the only article in Directive 2012/13/EU, which focuses on the right of access to the case materials. The central question is whether Art. 7 should be applied differently to the pre-trial proceedings as compared to the trial. As concerns Art. 7(1), obviously, it applies to both stages: someone can be arrested or detained both before and after the case reaches the trial. However, it is unclear from the wording of Art. 7(2) and (3) whether the general right of access to the case materials (unrelated to arrest or detention) also applies to the pre-trial procedural stages (such as pre-trial suspect interrogations), and to what extent. In *Kolev*, the CJEU did not clarify these issues either, as this case focuses on the latest, not on the earliest point of the proceedings when access should be granted.[6] There are also other ambiguities of wording of Art. 7 in the context of pre-trial proceedings. For instance, the formulation of derogations in Art. 7(4) allows for some variance in interpretation depending on the national specifics, especially the part related to the prejudice to an ongoing investigation. These problems are discussed in detail below, as they form a basis for making an argument for requesting preliminary references to the CJEU.

II. The Right of Access to the Case Materials upon Challenge of Arrest or Detention: Emerging Questions

Although it is clear from Art. 7(1) that it applies at any stage of criminal proceedings upon arrest or detention, two questions remain open.

First, which documents are essential for challenging effectively the lawfulness of the arrest or detention? According to the ECtHR, reasonable suspicion is a condition *sine qua non* for the lawfulness of the arrest or detention, but with the lapse of time it is not enough to justify continued detention.[7] With the lapse of time other valid grounds must exist to justify the deprivation of liberty, such as the risk of absconding or tampering with evidence.[8] When it comes to challenging the lawfulness of the detention, the ECtHR requires that

> "the detainee must be given an opportunity effectively to challenge the basis of the allegations against him [...]. This may require the court to hear witnesses whose testimony appears prima facie to have a material bearing on the continuing lawfulness of the detention [...]. It may also require that the detainee or his representative be given access to documents in the case file which form the basis of the prosecution case against him […]."[9]

Here, access to the case materials provides the detainee with information about the evidence, which supports the law enforcement agents' claim about the existence of reasonable suspicion that he has committed an offence, and (if applicable) about the additional ground(s) for continued detention. Based on this information, the detainee can challenge these claims, and submit evidence if necessary. The explanatory memorandum of the Commission proposal on the Directive calls it a "limited access to the case-file" which "ensures the fairness of pre-trial proceedings concerning the lawfulness of arrest and detention."[10] In this context, a number of questions arise: To what extent is the access limited? Does it cover all evidence the prosecution has against the suspect? If not, who decides, and based on what criteria, which evidence should be revealed to the defence, given that the lawyer – who would be best suited to assess which evidence is essential for challenging the arrest or detention effectively – is not given access to the complete case materials? And how, if at all, could the lawyer or the suspect control whether all such evidence has been disclosed? Does "limited access to the case-file" also cover exculpatory evidence in the possession of the prosecution?[11] These questions are very closely related to the next question concerning the possible derogations of Art. 7(1).

When it comes to determining which evidence is essential for challenging the arrest or detention, evidently, national peculiarities must be considered when making individual decisions about the scope of access to case materials, because the laws of Member States may provide for different grounds for continued detention (as long as they are in line with Art. 5(3) ECHR and the respective case law).[12] However, the question is to what extent should national differences be taken into account? What if, for instance, national law defines the moment from which 'reasonable suspicion' exists (and the criminal proceedings begin) differently than the respective ECtHR case law?[13] In Bulgaria for instance, the first 24 hours of police detention, or police arrest, of someone suspected of having committed a crime are not considered part of the criminal proceedings,[14] and therefore detention orders (which do not contain information about the factual grounds for arrest) might be handed out to suspects hours after the actual detention. Is this situation compatible with Art. 7(1)? Nevertheless, the questions we raised above about the interpretation of Art. 7(1) are more general, and therefore they need fundamental answers given by the CJEU. In addition, as we will demonstrate immediately below, the questions on the interpretation of Art. 7(1) and (4) are interrelated, and therefore must be analysed jointly.

This leads us to the second question, i.e. does Art. 7(4) apply in cases where access to the case materials must be granted in accordance with Art. 7(1), i.e. can Art. 7(1) be derogated by

Art. 7(4)? One might consider several arguments against and for the derogation. On the one hand, literal interpretation of Art. 7(1) and (4), which is one of the dominant interpretation techniques of the CJEU,[15] seems to suggest that Art. 7(1) cannot be derogated by Art. 7(4). As Art. 7(4) makes reference only to Art. 7(2) and (3), it implies that it does not apply to any other paragraphs of Art. 7. This is also backed by historic interpretation (even though the CJEU does not often rely on it), because the explanatory memorandum of the Commission proposal to the Directive makes reference to possible derogations from access to the case materials only in relation to access for the preparation of the trial.[16] Also, this viewpoint is also shared by legal academic literature[17]. On the other hand, contextual interpretation (also often used by the CJEU)[18] suggests that Art. 7(1) may be derogated on the grounds provided in Art. 7(4). More precisely, recital 42 of Directive 2012/13/EU states that "[t]he provisions of this Directive that correspond to rights guaranteed by the ECHR should be interpreted and implemented consistently with those rights, as interpreted in the case-law of the European Court of Human Rights". Furthermore, according to recital 32 "[r]estrictions on such access should be interpreted strictly and in accordance with the principle of the right to a fair trial under the ECHR and as interpreted by the case-law of the European Court of Human Rights." According to the ECtHR, the right of access to the case materials upon arrest or detention can be restricted if it is strictly necessary, for example to protect the safety and security of third parties (witnesses or victims).[19] In any case, the contextual interpretation relies on recitals 32 and 42 of the Directive, as these recitals – read in conjunction with Art. 7(1) – limit the right provided in this paragraph.

Because CJEU case law emphasises that recitals should not limit or contradict the rights stipulated in the actual provisions of a directive,[20] it may be argued that contextual interpretation is not appropriate to solve the given interpretation question. If the outcome of literal interpretation is however that both lawyers and suspects (as the holders of the rights) should be granted access to all materials of the case that are essential to challenge the arrest or detention, this inevitably raises the question on how to protect important values, such as privacy or personal safety? For instance, what if there is a real risk that disclosing the name(s) or whereabouts of (a) certain witness(es), or the (full) content of their statements to the suspect, might cause an attempt on the part of the suspect to influence their testimony and/or threaten their privacy or safety? This question is definitely worth raising with the CJEU. Here, an additional question to be addressed is whether procedures in some Member States enabling lawyers to see the materials but not to share them with their clients are compatible with Art. 7(1).[21]

Additionally, the timing of disclosure might also raise some issues. According to recital 30, the necessary documents must be made available to the defence "at the latest before a competent judicial authority is called to decide upon the lawfulness of the arrest or detention […], and in due time to allow the effective exercise of the right to challenge the lawfulness of the arrest or detention". But what does this really mean? How much time should the defence be granted before the judicial authority makes such decision, considering that the aim of adequate preparation is the effective exercise of the defence rights?

III. The General Right of Access to the Case Materials in Pre-Trial Proceedings: Does It Exist and to What Extent?

As already stated above, Art. 7(2) and (3) leave open the question whether access to the case materials (at least to some extent) has to be granted in pre-trial proceedings for other purposes than challenging an arrest or detention. The initial proposal for Directive 2012/13/EU envisaged that access to the case materials should be granted once the investigation of the criminal offence is concluded (then Art. 7(2)). Under this formulation, Member States would need to provide full access to the case materials (unless the public safety and security grounds for derogating from such access existed) upon the conclusion of the pre-trial investigation, but did not encourage them to provide access earlier – other than for the purpose of challenging an arrest or detention, which is a separate obligation provided in Art. 7(1).

The current wording of Art. 7(3) defines the latest possible stage of the proceedings when access should be granted – i.e. "upon submission of the merits of the accusation to the judgment of a court" –,[22] but adds that access should be granted "in due time to allow the effective exercise of the rights of the defence." According to Art. 7(2), such access is necessary "in order to safeguard the fairness of the proceedings and to prepare the defence". In this way, Art. 7(3) calls for variation of practices in the Member States. It might be that some states choose to provide access to the case material exactly at the latest possible stage of the proceedings foreseen by the Directive, but it might also be that some decide that for the effective preparation and exercise of the defence it is essential to provide access already in the earlier stages (during or in the end of pre-trial investigation). This decision is most likely to be made based on national laws and practices. For instance, those Member States that encourage the practice of negotiations in criminal proceedings towards out-of-court settlements are more likely to encourage early disclosure of the evidence in the possession of the prosecution to enhance such practice.[23] In addition, in those Member States where

lawyers are expected to actively participate in pre-trial proceedings (e.g. via active participation in suspect interrogations or the gathering of evidence), counsel might encounter less difficulties convincing authorities that in order to fulfil their duties effectively, they need to be informed of the evidence in the prosecution's possession.

But are these differences acceptable in the light of Art. 7(2) and (3) of the Directive? If, for instance, in Member State A this provision is interpreted in a way that the right of access to the case materials is provided for suspects who have not been arrested or detained only shortly before the court proceedings, and in Member State B already when counsel prepares for the initial interrogation, would suspects be equally able to exercise their defence rights effectively in both Member States? Is Member State A following the minimum standards, which Member State B has decided to depart from towards a higher standard of protection? Or is Member State A falling below minimum standards? Should the right of access to the case materials at an earlier stage than the referral of the case to court in Member State B be really left open for a case-by-case decision with an option for the national courts to make a preliminary reference to the CJEU? Or should there be a common EU-wide approach concerning the question at which stages of pre-trial criminal proceedings the right of access to the case materials is essential for the effective exercise of the defence rights?[24] We believe that this is a subject worth forwarding to the CJEU to clarify.

Art. 7(2) provides for the right of full access to the case materials – "to all material evidence in the possession of the competent authorities, whether for or against suspects or accused persons"[25] – at the latest when the case reaches the court (Art. 7(3): "upon submission of the merits of the accusation to the judgment of a court"). If these paragraphs are to be interpreted in a manner that they grant access to the case materials also at the pre-trial stages of the proceedings if necessary for exercising effective defence rights, the question arises whether full or partial access should be given (and would differences between Member States be acceptable)? There are two viable alternatives. First, it may be argued that because the aim of granting access is to "allow the effective exercise of the rights of the defence", the extent of access to the case materials depends on the stage and type of the proceedings in which it is granted. For instance, participation in the proceedings for an out-of-court settlement seems to require full prior knowledge of the existing evidence. In this first scenario, the decision on how much to reveal to the defence would belong to the competent authorities and would depend on their understanding of what is an "effective exercise of the rights of the defence" and how granting access to the case materials contributes to it. In addition, even when the competent authority concludes that granting access to evidence would contribute to the effective defence, it could still refuse such access based on Art. 7(4). Second and alternatively, it may be argued that in principle, full access to the case materials should be granted because full knowledge of the file is necessary for effective exercise of the defence *per se*, unless grounds for derogation under Art. 7(4) exist, which makes the right of access potentially more extensive, than in the first scenario.

The interpretation of derogations provided in Art. 7(4) raises further questions. There are two distinct grounds for derogation in Art. 7(4): the protection of third parties ("access may lead to a serious threat to the life or the fundamental rights of another person") and an important public interest ("access could prejudice an ongoing investigation or seriously harm the national security of the Member States"). In the initial draft of the Directive, the first ground was formulated almost identically compared to the adopted version, but the second ground was conceived much narrower, as it stated that access to certain materials could be refused if such access may seriously harm the internal security of the Member State.[26] In the finally adopted version, national security is mentioned together with the interests of the ongoing investigations (as implied in "prejudice an ongoing investigation") as possible examples of what may be considered an "important public interest" (implying that these two examples are non-exhaustive).

The 'life and limb' clause is also provided as a ground for derogation from the right of access to a lawyer in Art. 3(6)(a) of Directive 2013/48/EU.[27] However, there is no 'important public interest' clause, as the second ground for derogating the right of access to a lawyer is formulated as the need for investigating authorities to "prevent substantial jeopardy to criminal proceedings" (Art. 3(6)(a) of Directive 2013/48/EU). As a result, Art. 3(6)(b) of Directive 2013/48/EU is much more precise than Art. 7(4). In the latter, the public interest clause with reference to the interests of the ongoing investigation leaves a wide margin of interpretation for the Member States, which may use this ground excessively to the prejudice of defence rights.[28] The need to secure an effective conduct of criminal proceedings is more frequently invoked with regard to the pre-trial stage of the criminal proceedings than to the trial itself. Therefore, if Art. 7(2) and (3) are interpreted in a manner that they apply to pre-trial investigations (at least to some extent), national authorities can block this access due to the very vague wording of Art. 7(4), which would turn the right to early access to case materials into more of an exception than a rule. Consequently, we believe that here further guidance from the CJEU is needed in order to ensure effective protection of the rights of defence.

IV. Conclusions

The issue of pre-trial access to the case materials is delicate. *Packer* observed that any norm-setting in the area of criminal process aims at achieving a certain balance between two types of competing values: due process and crime control.[29] Likewise, the conflict between due process and crime control values underlies the debate about the right of early access to the case materials. On the one hand, an unlimited right of access from the initial stages of criminal proceedings would ensure maximum protection of due process values. Early access to the case materials is crucial for the effective conduct of defence. It provides counsel with an opportunity to choose tactics for interrogation (in general terms, whether to advise the suspect to remain silent or give statements), to request the gathering of evidence from the authorities (or to gather evidence himself or herself if national law permits), and to decide on the overall strategy of defence (e.g. whether to seek an out-of-court settlement, to proceed to trial etc.). These opportunities contribute to the principle of equality of arms, which has been embraced by the ECtHR not only as a principle that applies in trial, but also in pre-trial proceedings.[30] On the other hand, imposing restrictions or derogations from the right of access to the case materials, and/or delaying the moment when such access should be granted, would ensure optimal protection of crime control values. Thus, the earlier the suspect and his/her lawyer are granted access to the case materials, the greater the potential risk of prejudice to the ongoing investigation. Pre-trial investigations, especially at the early stages, are vulnerable to the risk of suspects tampering with evidence, as well as threatening witnesses. Therefore, next to compromising the integrity of criminal investigations, unlimited early access to the case materials may also jeopardise the safety of third parties.

All these considerations could be found in Art. 7(4) of Directive 2012/13/EU that provides derogations from the right of (unlimited) access to the case materials in criminal proceedings. However, there is evidence that derogations from pre-trial access to case materials are used too extensively in the EU Member States.[31] One of the reasons for this might be that law enforcement authorities still seem to believe that the best way to solve crimes is to conduct investigations first by keeping the details of the investigation confidential, after which the suspect or the accused can be confronted with the entire body of evidence against him. We believe that the contemporary understanding of equality of arms in pre-trial proceedings precludes this approach. With this article we encourage practitioners to contest these practices by raising questions of interpretation of Art. 7 of Directive 2012/13/EU in the context of the principle of adversarial proceedings and the principle of equality of arms in pre-trial proceedings, which could be a source of inspiration for making preliminary references to the CJEU.

---

* This article is based on the research conducted for: A. Pivaty and A. Soo, "Article 7 of the Directive 2012/13/EU on the Right to Information in Criminal Proceedings: A Missed Opportunity to Ensure Equality of Arms in Pre-Trial Proceedings?", forthcoming in the journal "European Journal of Crime, Criminal Law and Criminal Justice" (issue 2/2019). It develops the ideas expressed in the original article on a more practical level, which we hope to be of added value for practitioners interested in EU law on criminal procedure and procedural rights. We would like to thank Laure Baudrihaye-Gérard for her most valuable ideas and comments, which helped us improve this article a lot.

1 *O.J.* L 142, 1.6.2012, 1.

2 Art. 7(1) of Directive 2012/13/EU: "Where a person is arrested and detained at any stage of the criminal proceedings, Member States shall ensure that documents related to the specific case in the possession of the competent authorities which are essential to challenging effectively, in accordance with national law, the lawfulness of the arrest or detention, are made available to arrested persons or to their lawyers."

3 Art. 7(2) of Directive 2012/13/EU: "Member States shall ensure that access is granted at least to all material evidence in the possession of the competent authorities, whether for or against suspects or accused persons, to those persons or their lawyers in order to safeguard the fairness of the proceedings and to prepare the defence." Art. 7(3): "Without prejudice to paragraph 1, access to the materials referred to in paragraph 2 shall be granted 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. Where further material evidence comes into the possession of the competent authorities, access shall be granted to it in due time to allow for it to be considered."

4 Art. 7(4) of Directive 2012/13/EU: "By way of derogation from paragraphs 2 and 3, provided that this does not prejudice the right to a fair trial, access to certain materials may be refused if such access may lead to a serious threat to the life or the fundamental rights of another person or if such refusal is strictly necessary to safeguard an important public interest, such as in cases where access could prejudice an ongoing investigation or seriously harm the national security of the Member State in which the criminal proceedings are instituted. Member States shall ensure that, in accordance with procedures in national law, a decision to refuse access to certain materials in accordance with this paragraph is taken by a judicial authority or is at least subject to judicial review."

5 CJEU, 5 June 2018, case C- 612/15, *Criminal proceedings against Nikolay Kolev and Others*.

6 Ibid, paras. 90–100.

7 ECtHR, 12 May 2015, *Magee and others v. the UK*, Appl. nos. 26289/12 et al., para. 88.

8 ECtHR, 28 July 2005, *Czarnecki v. Poland*, Appl. no. 75112/01, para. 37.

9 ECtHR, 19 February 2009, *A. and others v. the UK*, Appl. no. 3455/05, para. 204.

10 European Commission, "Proposal for a Directive of the European Parliament and of the Council on the right to information in criminal proceedings", COM(2010) 392 final, p. 9.

11 In *A. and others v. the UK* (*op. cit.* (n. 9)) the ECtHR noted that, "while the right to a fair criminal trial under Article 6 includes a right to disclosure

Anneli Soo
Humboldt Experienced Researcher, University of Cologne and Max Planck Institute for Foreign and International Criminal Law (2018–2019)

Anna Pivaty
Researcher, Maastricht University

of all material evidence in the possession of the prosecution, both for and against the accused, the Court has held that it might sometimes be necessary to withhold certain evidence from the defence on public-interest grounds." (para. 206) It did not use the phrase "evidence for and against the accused" in the context of challenging arrest or detention. However, it stated that, "the proceedings must be adversarial and must always ensure 'equality of arms' between the parties" (para. 204), and required that, "the detainee must be given an opportunity effectively to challenge the basis of the allegations against him." (ibid) The principle of equality of arms is not honored and the opportunity to effectively challenge the basis of the allegation is not given to the detainee if exculpatory evidence is concealed.

12 Despite the extensive existing Strasbourg case law on the lawful basis for detention, Fair Trials has reported quite remarkable differences concerning the grounds for pre-trial detention among the Member States. Fair Trials, "A Measure of Last Resort? The practice of pre-trial detention decision-making in the EU, 2016", <https://www.fairtrials.org/wp-content/uploads/A-Measure-of-Last-Resort-Full-Version.pdf>, pp. 18–20, accessed 1 February 2019.

13 Reasonable suspicion is defined by the ECtHR as "the existence of facts or information which would satisfy an objective observer that the person concerned may have committed offence". See e.g. ECtHR, 30 August 1990, *Fox, Campbell and Hartley v. the UK*, Appl. nos. 12244/86; 12245/86; 12383/86, para. 32.

14 See Y. Grozev, "National Approaches to Effective Defence: Bulgaria", in: E. Cape and Z. Namoradze (eds.), *Effective Criminal Defence in Eastern Europe*, 2012, p. 104.

15 CJEU, 28 June 2007, case C-467/05, *Criminal proceedings against Giovanni Dell'Orto*, para. 54.

16 COM(2010) 392 final, *op. cit.* (n. 10), p. 9.

17 S. Allegrezza and V. Covolo, "The Directive 2012/13/EU on the Right to Information in Criminal Proceedings: Status Quo or Step Forward?", in: Z. Durdevic and E. Ivicevic Karas (eds.), European Criminal Procedure Law in Service of Protection of the Union Financial Interests: State of Play and Challenges, 2016, p. 47; A. Tsagkalidis, "Directive 2012/13/EU on the Right to Information in Criminal Proceedings", ERA, Krakow, 2 March 2017, <http://www.era-comm.eu/procedural_safeguards/kiosk/pdf/2017/Article_Right_to_Information.pdf>, p. 13, accessed 1 February 2019.

18 Cf., for instance, CJEU, *Criminal proceedings against Giovanni Dell'Orto*, *op. cit.* (n. 15), paras. 55–57.

19 ECtHR, *A. and others v. the UK*, *op. cit.* (n. 9), para. 205.

20 CJEU, 24 November 2005, case C-136/04, *Deutsches Milch-Kontor GmbH v. Hauptzollamt Hamburg-Jonas*, para. 32.

21 The ECtHR has accepted these procedures on specific conditions: ECtHR, *A. and others v. the UK*, *op. cit.* (n. 9), paras. 209–211.

22 In *Kolev*, the CJEU stated that the requirements of Article 7(3) are met if access to the case materials has been granted "after the lodging before the court of the indictment that initiates the trial stage of the proceedings, but before that court begins to examine the merits of the charges and before the commencement of any hearing of argument by that court, and after the commencement of that hearing but before the stage of deliberation where new evidence is placed in the file in the course of proceedings, provided that all necessary measures are taken by the court in order to ensure respect for the rights of the defence and the fairness of the proceedings." CJEU, *Criminal proceedings against Nikolay Kolev and Others, op. cit.* (n. 5), para. 100.

23 However, Fair Trials has reported that such enhanced or early access to the case materials is often not provided, and therefore this situation needs improvement. Fair Trials, "The Disappearing Trial. Towards a rights-based approach to trial waiver systems", <https://www.fairtrials.org/sites/default/files/publication_pdf/Report-The-Disappearing-Trial.pdf>, pp. 80–81, accessed 10 March 2019.

24 The CJEU hinted in *Kolev* that the latest point in time for granting access to case materials may vary depending on the type of procedure by stating that "as a general rule and without prejudice, in some cases, to special or simplified procedures, that that disclosure should take place, and that the opportunity to have access to the case materials should be afforded, no later than the point in time when the hearing of argument on the merits of the charges in fact commences before the court that has jurisdiction to give a ruling on the merits." (CJEU, *Criminal proceedings against Nikolay Kolev and Others, op. cit.* (n. 5), para. 92).

25 Here it is important to notice that the Directive limits disclosure to "material evidence", but this may lead to a situation in which material relevant for the defence remains unrevealed as it is not used for the purposes of the court proceedings. See the recent rape cases in the UK in which undisclosed unused materials contained exculpatory evidence, leading to the enquiry and report by the Attorney General. Attorney General's Office, "Review of the efficiency and effectiveness of disclosure in the criminal justice system. November 2018", <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756436/Attorney_General_s_Disclosure_Review.pdf>, accessed 10 March 2019.

26 European Commission, "Proposal for a Directive of the European Parliament and of the Council on the right to information in criminal proceedings", *op. cit.* (n. 10), p. 9.

27 Directive 2013/48/EU 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, *O.J.* L 294, 6.11.2013, 1.

28 The excessive use of the 'interest of investigation' clause has been reported by Fair Trials (Fair Trials, "Legal Experts Advisory Panel Survey Report: Access to the Case File, March 2015", <https://www.fairtrials.org/wp-content/uploads/Access-to-file-report-FINAL.pdf>, pp. 16–17, 19, accessed 1 February 2019) and the European Union Agency for Fundamental Rights (FRA), "Rights of Suspected and Accused Persons Across the EU: Translation, Interpretation and Information", 2016, p. 78 and figure 7 on p. 79).

29 H.L. Packer, *The Limits of the Criminal Sanction*, 1968, pp. 149–173.

30 ECtHR, 24 November 1993, *Imbrioscia v. Switzerland*, Appl. no. 13972/88, para. 36; ECtHR, 30 March 1989, *Lamy v. Belgium*, Appl. no. 10444/83, para. 29.

31 Fair Trials, "Legal Experts Advisory Panel Survey Report", *op. cit.* (n. 28); FRA, "Rights of Suspected and Accused Persons Across the EU", *op. cit.* (n. 28).

Fighting Terrorism through the European Public Prosecutor's Office (EPPO)?

What future for the EPPO in the EU's Criminal Policy?

Adam Juszczak and Elisa Sason

The EPPO was established by Regulation 2017/1939, which entered into force on 20 November 2017, under enhanced cooperation to fight crimes affecting the Union budget. The Office is currently in the set-up phase with the aim of becoming operational at the end of 2020. On 12 September 2018, the Commission published a Communication on the extension of the EPPO's competences to cross-border terrorist crimes and invited the European Council to take this initiative forward at the informal summit in Sibiu on 9 May 2019. As a single, decentralised European prosecution office, the EPPO could become an effective tool in investigating, prosecuting and bringing to judgement terrorist crimes and add a European dimension to the current efforts. Compared to the present horizontal, multinational approach, the EPPO would create a vertical, European relationship amongst the Member States and Union actors. This could be a decisive qualitative improvement, which would help overcoming the divergences of effective investigation and prosecution of terrorist crimes across the EU.

This article outlines the key aspects of the Communication, touches upon the procedural/legal steps needed for an extension of the EPPO's competences, and discusses the potential legal and practical implications of such an extension. It sets out which aspects demand particular attention prior to a decision on an extension of the competences of the EPPO, thereby stressing that justice and security are inextricably linked and have to be looked at together. The authors point out that a narrower and more targeted approach, such as a gradual extension of the EPPO's competences to financial crimes, organised crime or cybercrime could also be envisaged, while at a later stage other types of crimes, such as trafficking in human beings, trafficking in arms and eventually cross-border terrorist crimes, could be included.

I. Introduction

On 9 May 2019, the European Council met in Sibiu, Romania, to discuss the future of Europe. This informal summit was the culmination of the process launched by President *Juncker* in his 2017 State of the Union address,[1] which included a roadmap[2] detailing the main steps towards a more united, stronger and more democratic EU. A fundamental role in this respect concerns the EU's next strategic agenda for 2019 to 2024. One of the key aspects in this context relates to ensuring the security of EU citizens and in particular the fight against terrorism.[3] For the purpose of this summit, the Commission put forward an initiative[4] on an extension of the competence of the newly established European Public Prosecutor's Office[5] (hereinafter "Communication").

While the Commission's White Paper on the future of Europe[6] reflects about the challenges that the Union is facing and in that context about an EU-wide prosecution office to become competent for a range of crimes in general terms, the initiative on the extension of the competences of the European Public Prosecutor's Office (hereinafter "EPPO") has its origins primarily in President Juncker's 2017 State of the Union address, where the EPPO is seen as a potentially effective tool to fight cross-border terrorist crimes.

Although it is not the first time that the idea to empower the future EPPO to fight terrorist crimes was voiced,[7] President Juncker's remark came rather unexpectedly, given that at that time the Council was still due to adopt the Regulation on the establishment of the EPPO (hereinafter "EPPO Regulation"), which gives the EPPO competence over crimes affecting the financial interests of the Union. Moreover, not all Member States wished to participate, which is why the EPPO Regulation was adopted under enhanced cooperation on 12 October 2017, after more than four years of complex negotiations. The EPPO Regulation also foresees a set-up phase of at least three years, meaning that the EPPO is currently in the midst of its build-up process and cannot take up its functions before the end of 2020.[8]

The Communication forms part of a broader package of ambitious measures complementing the Security Union and thus enhancing the security of the European citizens. It explores the idea of tasking the EPPO with investigating, prosecuting and bringing to judgement terrorist crimes – with a 2025 per-

spective.[9] These reflections aim at launching a discussion on a range of questions that need to be addressed prior to taking a decision on the extension of the EPPO's competence to terrorist crimes.

The reactions to the Communication from the side of national parliaments or national governments[10] were rather mixed, some welcoming the initiative, others expressing their concerns. In general, it was stated that this initiative came too early and further analysis on this equally complex and sensitive matter was required.

This article will outline the key aspects of the Communication (III.), touch upon the procedural/legal steps needed for an extension of the EPPO's competences (IV.), discuss potential legal and practical implications of such an extension (V.), and conclude with a number of observations (VI.). Beforehand, this article will recall the main features of the EPPO in its current design[11] and provide a brief state of play of its set-up process (II.).

II. The EPPO *de lege lata* and State of Play of the Set-Up Process

1. The EPPO in a nutshell

The EPPO is an independent European prosecution office created to fight crimes affecting the financial interests of the Union, as defined in Directive 2017/1371 ("PIF Directive").[12] This includes crimes, such as fraud, corruption, money laundering or complex VAT carousels, as well as crimes related to the participation in a criminal organisation,[13] if the focus is to commit crimes that affect the financial interests of the Union, and, eventually, any other criminal offence that is inextricably linked to a crime affecting the financial interests of the Union.[14]

The EPPO was established under enhanced cooperation in accordance with the procedure provided in Art. 86 of the Treaty on the Functioning of the European Union (TFEU), with currently 22 participating[15] Member States.[16] On 3 April 2019, Sweden's Prime Minister, *Stefan Löfven*, announced in the European Parliament that the Swedish Government will propose to the Swedish Parliament that Sweden joins the EPPO, although there is no indication when this would happen.[17]

The EPPO's structure consists of two levels. The central level is located at the EPPO's seat in Luxembourg, where the European Chief Prosecutor and European Prosecutors from each participating Member State – organised in Permanent Chambers – monitor and supervise the investigations and prosecutions carried out by European Delegated Prosecutors located in the Member States.

In this way, the EPPO will operate directly across all participating Member States, allowing for direct action and immediate information exchange, coordinated police investigations, fast freezing and seizure of assets and ordering of arrests across the EU. Moreover, the EPPO will operate on the basis of a permanent structure, i.e. there will be no need for *ad hoc* Joint Investigation Teams (JITs) or mutual legal assistance requests.

The EPPO will also possess a unique overview over cross-border criminal activity in the Union and beyond falling within the remit of its material, territorial and personal[18] competence. This will also enable the EPPO to develop a common investigation and prosecution strategy.

The Office will work hand in hand with national law enforcement authorities and exercise the function of prosecutor in the competent courts of the participating Member States. In carrying out its mandate, the EPPO will also closely cooperate with EU agencies and bodies, such as Eurojust, Europol, and the European Anti-Fraud Office (OLAF).

As the only prosecution body at Union level, the EPPO seems also ideally placed to cooperate with third countries, thereby building on the provisions of the EPPO Regulation related to international cooperation as well as the legal framework that will be created on that basis.[19] Once operational, the EPPO will become an integral part of the Union's security architecture and draw upon the existing experience and best practices at national and EU level.

2. State of play of the set-up process

Art. 20 of the EPPO Regulation provides that the Commission is responsible for the establishment and initial administrative operation of the EPPO, until the latter has the capacity to implement its own budget. To that end, the Commission has taken a wide range of preparatory steps towards setting up the EPPO, in close consultation with a group of experts composed of representatives of the participating Member States (EPPO Expert Group).[20]

This preparatory work relates to the recruitment of the key EPPO staff, in particular the European Chief Prosecutor and the European Prosecutors,[21] the development of the EPPO Case Management System, the premises for the seat of the future EPPO in Luxembourg, the preparation of the 2019 and 2020 budgets, and many other logistical, administrative, financial and legal matters. The Commission has consulted the EPPO Expert Group on these matters and in this context also discussed the necessary adaptations to be made in national law following the adoption of the EPPO Regulation.[22]

Currently the Council and the Parliament are in the process of agreeing on a common candidate for the post of European Chief Prosecutor. As regards the selection procedure of the European Prosecutors, the Commission invited the Member States to start their national selection procedure and nominate three candidates per Member State by the end of March 2019. The selection procedure of the European Prosecutors is currently also ongoing and the selection panel referred to in Article 14(3) of the EPPO Regulation[23] will hear the nominees and provide reasoned opinions on the 66 candidates,[24] in order for the Council to appoint the European Prosecutors from the 22 participating Member States by the end of 2019. According to the Commission's timelines, the EPPO shall become functional at the end of 2020.

III. Extension of the EPPO Competence: Key Aspects of the Commission Communication

The Commission presented the above-mentioned initiative to extend the competences of the EPPO as its vision of establishing a comprehensive and structured Union response to the threat of terrorism. This should include the investigation and prosecution of terrorist offences across the Union.

While acknowledging that decisive action and measures have already been taken in the fight against terrorism,[25] the Communication sets out a number of gaps in the investigation and prosecution of cross-border terrorist crime in the EU, which, in the Commission's view, have not yet been addressed within the existing framework. The Communication subsequently outlines how the EPPO, as a novel EU approach, could address these gaps. The identified gaps relate to the following aspects:

- Fragmentation of terrorist crime investigations at the national level (below 1.);
- Deficient sharing of information (below 2.);
- Disintegrated approach in the investigation and prosecution phases (below 3.);
- Potential conflicts of jurisdiction (below 4.).

1. Fragmentation of terrorist crime investigations at the national level

The first gap identified by the Commission relates to the fact that national authorities are exclusively responsible for investigating, prosecuting and bringing to judgement terrorist crimes, although these crimes very often have a cross-border nature. The result is a variety of different national approaches in the investigation and prosecution of terrorist crimes, accompanied by a deficient exchange of case-related information and lack of coordination/cooperation between the authorities of different Member States.

The Communication supports this view by making reference to the growing caseload of Eurojust in the area of terrorist crimes, stressing that cases are being investigated and prosecuted in parallel and in isolation in several Member States. In addition, the Communication underlines that both Eurojust[26] and Europol[27] primarily support the national authorities and are also not equipped with the required powers to proactively carry out coordinated prosecutions at the EU level. The Commission then outlines how the EPPO could provide a comprehensive Union response to enhance the fight against cross-border terrorist crimes. Particularly, the EPPO as a single office acting through the European Delegated Prosecutors, who are embedded in the national legal systems, could bridge the gaps in the national systems and provide better cooperation within and between the Member States at the EU level.

2. Deficient sharing of information

The timely sharing of information is important in any criminal investigation, yet crucial in terrorist crimes, which require immediate and targeted action by all law enforcement and judicial authorities. By obtaining information directly and through ordering or requesting the collection of relevant evidence, the EPPO may be in a central position to react to terrorist offences across the EU, as well as to cooperate with third countries or international organisations as the entity in charge.

3. Disintegrated approach in the investigation and prosecution phases

The Communication further points to the lack of a central authority at Union level, with the ability to direct both the investigation and prosecution phases of cross-border terrorist cases. Such a central authority would provide a smooth cooperation mechanism between all national and Union authorities involved and would operate in a far more efficient and effective manner than is the case today. According to the Communication, the EPPO would be such a central authority allowing for a more connected and coordinated investigation and prosecution approach. In this way, the EPPO could also tackle existing shortcomings following from parallel and fragmented investigations/prosecutions in terrorist cases.

4. Potential conflicts of jurisdiction

Lastly, the Communication refers to potential risks of conflicts of jurisdiction, which may occur in situations where several affected Member States want to exercise jurisdiction in relation to the same terrorist offence on different grounds, for ex-

ample the victim's or offender's nationality or territorial competence. The Communication underlines that in cross-border terrorist cases, there is a specific need for an adequate Union mechanism, also in view of avoiding problems related to the *ne bis in idem* principle.

Against this background, the Commission argues that the EPPO would be able to ensure a coherent and effective approach in the prosecution of terrorist crimes. Given its nature as the only Union-level actor to decide on the basis of objective criteria where to bring a case to court, the EPPO could prevent or reduce possible conflicts of jurisdiction and thus avoid unnecessary litigation.

IV. Procedural and Legal Steps for an Extension of the Competences

The Communication only briefly touches upon the legal and procedural requirements for an extension of the EPPO's competences to cross-border terrorist crimes. The central provision is Art. 86(4) TFEU, which foresees a simplified Treaty amending procedure. An envisaged extension of the competences of the EPPO would need to take place in two steps.

As a first step, the European Council would need to adopt a decision amending paragraphs 1 and 2 of Art. 86 TFEU in order to extend the powers of the EPPO to include "serious crimes having a cross-border dimension" and as regards the perpetrators of, and accomplices in, serious crimes affecting more than one Member State. For that purpose the European Council would need to "act unanimously after obtaining the consent of the European Parliament and after consulting the Commission", whereby the term "unanimously" in Art. 86(4) TFEU refers to all EU Member States, and not only to those participating in the enhanced cooperation of the EPPO. This even includes the Member States, which do not, by virtue of Protocols 21 and 22, take part in the adoption of measures by the Council under Title V of Part Three of the TFEU, i.e. Denmark, Ireland, and – unless Brexit happens – also the UK.

The European Council may amend Art. 86(1) TFEU to extend the material competence of the EPPO to all, some or only one of the "serious crimes having a cross-border dimension". This notion includes the "particularly serious crime[s] with a cross-border dimension" referred to in Art. 83(1) TFEU and listed in the second subparagraph of this provision. It is hence legally possible to extend the competence only to one of those crimes, e.g. terrorism. Further to that, the amendments to Art. 86(1) and (2) TFEU would also need to reflect the additional requirement laid down in Art. 86(4) TFEU, according to which the EPPO's competence may only be extended in relation to serious crimes affecting "more than one Member State".

Although Art. 86(4) TFEU does not foresee that the European Council acts on a proposal from the Commission, this does not prevent the Commission from taking an initiative under Art. 17(1) of the Treaty on European Union (TEU). And indeed, the Commission put forward a draft European Council Decision, proposing the necessary amendments to paragraphs 1 and 2 of Art. 86 TFEU.[28]

As a second step, separate from the European Council's decision to amend Art. 86 TFEU, the EPPO Regulation would need to be modified accordingly so as to include the competence over cross-border terrorist crimes. Such amendment must, *inter alia*, take into account the requirement that more than one Member State needs to be affected, and introduce the possible adaptations that might be required for the EPPO's activities concerning terrorism being effective. In that legislative procedure, the principles of subsidiarity and proportionality will be examined.[29]

The circumstance that the current EPPO Regulation was adopted under enhanced cooperation raises a number of legal questions. The Communication outlines, for instance, that it would not be possible to have a "variable geometry" within the EPPO in a way that Member States would participate in different parts of its competence. According to Art. 86(4) TFEU, the decision of the European Council "to extend the powers of the European Public Prosecutor's Office" does not amount to the establishment of a new or second EPPO but to a modification of the competences of the existing EU body. Given that the EPPO was established by enhanced cooperation, the EPPO Regulation would have to be amended by all and for all the participating Member States. In addition, non-participating Member States that would join the EPPO at a later stage would have to participate in it as a whole, and could not limit their participation to a particular area of the EPPO's competence.

V. Implications of an Extension

Extending the EPPO's competence to cross-border terrorist crimes would demand an in-depth analysis of how and to which extent the current framework of the EPPO – which is tailor-made to combat crimes affecting the Union budget – would need to be adapted in order for the EPPO to fight these crimes as a single investigatory and prosecutorial office. Terrorism cases differ from other types of criminal cases due to their inherent degree of complexity and the need for quick and efficient multilateral action. Swift exchange of informa-

tion and evidence, accelerated execution of mutual legal assistance and extradition requests, European Arrest Warrants (EAWs) and European Investigation Orders (EIOs), as well as setting up Joint Investigation Teams (JITs) are crucial aspects for a successful operation of the EPPO in the field of terrorism. Investigations in terrorist crimes generally involve significant human, technical and logistical resources. Furthermore, it should be recalled that a European criminal procedure code does not exist and that the EPPO will need to rely to a great extent on national law in order to carry out its investigations and prosecutions.[30] The following remarks highlight the relevant areas, which would require a careful assessment in the event that the EPPO's mandate would be extended to include cross-border terrorist crimes. It is obvious that this list is not exhaustive.

1. Competence

With regard to the material competence of the EPPO, the Communication suggests a targeted extension by simply adding a new paragraph in Art. 22 of the EPPO Regulation, which would make reference to Artt. 3 to 13 and 14 of Directive 2017/541 on combatting terrorism.[31] The EPPO Regulation follows this approach for the PIF crimes currently falling within the EPPO's material competence.[32] The Communication further clarifies that the requirement from Art. 86(4) TFEU, namely that the crimes need to affect more than one Member State, could be accommodated under the definitions in the EPPO Regulation.

Whether such quick solution would indeed suffice or whether there would be a need for greater precision in formulating the competences in the area of cross-border terrorist crimes in the EPPO Regulation, so as to avoid potential conflicts of competences, legal uncertainties and frictions in the investigation and prosecution of these crimes, will require careful analysis.

This includes the question of the scope and limits of the elements of crime, including the cross-border element, e.g. whether this would include preparatory acts to have taken place in another EU Member State and if so which; whether accomplices need to be located and act in another country; or whether transnational money transfers need to have been made in support of or related to the terrorist act in order to constitute a cross-border terrorist crime; and eventually whether, by way of a broader approach, e.g. the nationality of victims should also become a constitutive element, etc. In the same direction, a terrorist act solely based on the motivation to replicate similar terrorist crimes that have taken place in another country could, as such, possibly fall outside the scope of cross-border terrorist crime.[33]

2. Structure and decision-making procedures

Similar considerations as above apply to the present structure of the EPPO. The involvement and the roles of the various actors of the EPPO, such as the European Chief Prosecutor, the European Prosecutors, the Permanent Chambers and the European Delegated Prosecutors, in the investigations and prosecutions need to be carefully analysed with a view to assess whether this structure would fit the purpose of investigating and prosecuting cross-border terrorist crimes. A greater empowerment of the European Chief Prosecutor and/or the European Prosecutors or a greater specialisation of the Permanent Chambers should be considered.[34] Moreover, the multi-layered structure of the EPPO, as foreseen in the EPPO Regulation, may also need to be revisited from the perspective of the decision-making procedures. This relates in particular to the division of decision-making powers between the Permanent Chambers and the European Delegated Prosecutors, and the role of the European Prosecutors in between these two.

3. Investigation measures

While the EPPO Regulation includes a comprehensive set of investigation measures, allowing the EPPO to efficiently tackle crimes affecting the Union budget, it will be necessary to assess whether the tools at the EPPO's disposal will suffice to fight terrorist crimes or whether additional measures would be required. Due to the complex and specific nature of terrorist crimes, it may be required to broaden the scope of the investigation measures that the European Delegated Prosecutors have at their disposal in EPPO investigations.

Art. 20 of Directive (EU) 2017/541 on combatting terrorism goes in this direction when it stipulates that Member States need "to ensure that effective investigative tools, such as those which are used in organised crime or other serious crime cases, are available to persons, units or services responsible for investigating or prosecuting" terrorist and terrorist-related offences. Accordingly, one could consider adding to or expanding the EPPO's powers to make use of certain investigation measures, such as interception of telecommunications, real-time surveillance measures, covert investigations, inspecting means of transport, identification measures and measures to track and control persons.

Enhancing the investigatory powers of the EPPO in order to include measures of specific relevance to carry out investigations and prosecutions into terrorist crimes would equally demand an assessment of the impact on the procedural rights of suspects and accused persons in such proceedings (see below under 5.).

4. Collection of evidence

Throughout the investigations and prosecutions carried out by the EPPO, the principle of free admissibility of evidence applies as an overarching element.[35] Evidence against the defendant presented by EPPO prosecutors to a national court cannot be denied admission on the ground that it was collected in another Member State. The trial court is, however, allowed to examine the admissibility of the evidence, so as to ensure that its admission is not incompatible with Member States' obligations to respect the fairness of the procedure, the rights of defence, or other rights of the defendants, as enshrined in the Charter of Fundamental Rights, in accordance with Art. 6 TEU. Whether and if so to which extent the principle of free admissibility of evidence should be further developed or strengthened in the event that the EPPO would investigate and prosecute terrorist crimes, requires further assessment. Should the free admissibility of evidence become the future principle of the EU's criminal policy? It is clear that the collection of evidence across borders within the EU is becoming more important and that prosecutors and judges are more and more relying on the evidence collected in other Member States. An EU instrument providing common standards on the collection, handling and transfer of evidence could be envisaged in the future. Such rules could be applied to certain procedures or certain types of evidence, for example e-evidence or forensic evidence.

5. Procedural rights in EPPO proceedings

The EPPO Regulation offers a wide protection for suspects and accused persons involved in EPPO investigations and prosecutions.[36] The EPPO's activities will be carried out in full compliance with the Charter of Fundamental Rights of the EU, including the right to a fair trial and the rights of defence.[37] Suspects and accused persons can rely, at a minimum, on the existing or new EU acquis, which includes the Directives concerning the rights of suspects and accused persons in criminal investigations, ranging from the right to interpretation and translation in criminal proceedings, over the right to information and access to the case file, the right of access to a lawyer, the right to remain silent and the right to be presumed innocent to the right to legal aid.[38] Moreover, suspects and accused persons as well as other persons involved in EPPO proceedings, may seek recourse to all procedural rights available under national law. The EPPO Regulation also includes the possibility to present evidence, appoint experts, hear witnesses, or request the EPPO to obtain such measures on behalf of the defence. All these rights would also be applicable to suspects and accused persons in possible EPPO investigations into cross-border terrorist offences. Given the serious nature of these crimes and the impact on legal proceedings, it is indispensable to assess whether and to which extent an enhancement of the rights for suspects and accused persons in EPPO proceedings focused on terrorism is indicated irrespective of a potential widening of the investigatory powers of the EPPO as elaborated above.

6. Information flows

An extension of the EPPO's competence to cross-border terrorist crimes would have an impact on various other areas. Such an extension would, on its own, not solve shortcomings in information and intelligence sharing in the investigation of terrorist crimes. Throughout its operations, the EPPO will need to rely on information from all available sources, including intelligence. Allowing the EPPO to fight cross-border terrorist crimes hence requires a comprehensive approach, including the development of common rules on various security-related matters, such as, rules on the collection and sharing of information, access to databases, and use of special investigation measures. In addition questions related to rules on detention and penitentiary as well as juvenile justice must be addressed and resolved.

The EPPO would need to be granted access to the relevant information held by national authorities, including Financial Intelligence Units, which deal with suspicious transactions involving the financing of terrorism, as well as immigration offices, asylum offices, or border security offices. The EPPO would also need to be granted access to relevant information held by Eurojust and Europol, either through the exchange of liaison officers or by way of direct and secure access to databases and registers or through a pooling of the relevant expertise and information. To that end, the interconnectivity possibilities between the EPPO's Case Management System and other IT systems, would need to be explored and further developed.

7. Security aspects

An important aspect in the above-mentioned context concerns security. Consideration is to be given to security standards, including physical and perimeter security of the EPPO and its staff, as well as to the secure treatment of intelligence or soft information for the purpose of criminal investigation, which would be of far greater relevance in the context of investigating and prosecuting cross-border terrorist crimes compared to PIF crimes. Allowing the EPPO to work with a wide range of information coming from different sources, including intelligence and whistleblowers, would also require that the EPPO Case Management System is adapted to safely processing such information.

8. Budgetary and staffing considerations

As outlined in the Communication, since the EPPO is currently competent for fighting crimes affecting the Union budget, any extension of the EPPO's mandate could have significant implications on the EPPO's budget and staffing. This does not only relate to an increased workload with the addition of a completely new area of competence but in particular also in relation to security, which may require additional (specialised) staff and technical solutions with a considerable financial impact. The extent of these implications depends also on the adaptations that would have to be made to the EPPO, e.g. the creation of a separate department within the EPPO or the introduction of specialised Permanent Chambers focused on fighting terrorist crimes. Any possible synergy effects stemming from the extension of the EPPO's mandate would need to be assessed accordingly.

9. Impact on national authorities and EU bodies, in particular Eurojust and Europol

An extension of the EPPO's competence to terrorist crimes would have an impact on the current tasks and roles of Europol and Eurojust, as well as on relevant national authorities. Establishing a close relationship between the EPPO and the other relevant actors, and generating synergies, would be prerequisites for the EPPO to become an essential part of the EU-wide approach to fighting terrorist crimes. One of the key questions to consider with respect to national authorities is which powers the EPPO would need to have in order to direct the work of national authorities in the area of security. It is of note that Art. 4(2) TEU, which specifies that national security remains the sole responsibility of the Member States, would need to be taken into consideration in this context.

The EPPO, Eurojust and Europol have different tasks and different mandates. While the EPPO will be a European investigating and prosecuting body, Eurojust is an agency supporting and strengthening the coordination of investigations and prosecutions and cooperation between the competent national authorities in relation to serious crime, including terrorist offences, affecting two or more Member States. Europol is the Union agency which supports and strengthens action by competent national police authorities and their mutual cooperation in preventing and combatting serious crime affecting two or more Member States, including terrorism.

Given the current tasks and practical experience of Eurojust and Europol in the area of fighting terrorism,[39] an extension of the EPPO's competences to terrorist crimes would have to be carefully assessed in order to avoid duplication of work and to ensure that resources are used in the most efficient way. New cooperation models between the various EU bodies would need to be established in order to create the desired synergy effects. This could include e.g. developing an effective crime analysis capability at EU level, which could be a significant advantage in the context of sharing information. In the same vein, it should be considered that the EPPO is empowered to instruct Europol to perform crime analysis for it.[40]

From a practical point of view, the existing tools available at both Eurojust and Europol play a crucial role in investigating and prosecuting terrorist crimes. What may appear to be a purely national case, may turn out to be a large multi-national criminal offence from the perspectives of Eurojust and Europol, although the powers of these two bodies are entirely different in nature compared to EPPO. In any case, the special tools of Eurojust and Europol are of great use in making the fight against terrorist crimes more effective and this is something the EPPO would greatly profit from.

Further synergies may be created through a functional proximity between Eurojust, Europol and the EPPO as far as the fight against cross-border terrorist crimes is concerned. An option in this context could be to build the EPPO on the broad mandate and experience of Eurojust in the area of fighting terrorist crimes, by allowing these two EU bodies cooperate as closely as needed and possible.[41] In the long term, the option of bringing Eurojust and the EPPO under one roof could also be envisaged.

VI. Conclusions

While the focus should ideally lie on preventing terrorist crimes, it is clear that terrorism cannot be addressed through prevention only – an absolute prevention of terrorism is not possible. Where prevention fails, an effective judicial response at prosecution level must be safeguarded. The Union needs to ensure an equal level of protection through preventive as well as prosecution measures.

The EPPO, as a single, decentralised European prosecution office, could become an effective tool in investigating, prosecuting and bringing to judgement terrorist crimes and add a European dimension to the current efforts. Compared to the present horizontal, multinational approach, the EPPO would create a vertical, European relationship amongst the Member States and Union actors. This could be a decisive qualitative improvement, which would help overcoming the divergences of effective investigation and prosecution of terrorist crimes across the EU.

The following features of the EPPO underpin that the Office would be well placed to effectively investigate and prosecute terrorist crimes:

- A decentralised structure, with the European Delegated Prosecutors embedded in the national systems of the Member States and working hand in hand with national law enforcement authorities;
- A central office able to develop a coherent prosecution policy to fight terrorist crimes and steer the investigations and prosecutions carried out by the European Delegated Prosecutors, while having a unique overview over the criminal activity across the Union;
- Close cooperation with EU actors, such as Eurojust and Europol.

Despite the added value the EPPO could bring, the Leaders at the summit in Sibiu on 9 May 2019 did not discuss this matter and did not decide in favour of an extension of the EPPO's competences to cross-border terrorist crimes.

There might be good reasons for allowing the EPPO, which is still in the process of being set up, to first settle into the existing judicial landscape and establish smooth cooperation with other EU actors, as well as with the national authorities, which will be vital for its functioning in practice, before taking a decision on extending its mandate. Any extension would require an in-depth analysis of the legal and practical requirements taking account of the political dimension. Lessons learned from the valuable work of Eurojust and Europol could feed into this.

The EPPO Regulation foresees that five years after the start of its operations, the Commission is required to submit an evaluation report on the implementation and impact of the EPPO Regulation, as well as on the effectiveness and efficiency of the EPPO and its working practices.[42] Awaiting this evaluation prior to taking a decision on extending the EPPO's mandate could also be envisaged, although such approach could be considered as not flexible enough and not suitable to tackle the immediate problems in the fight against terrorism.

For sure the Commission Communication has triggered a debate on this important subject at the political level as well as amongst practitioners and academics. It illustrates that security and justice aspects cannot be looked at separately, but holistically. It is also clear that the fight against cross-border terrorist crimes is resource intensive and the EU would need to ensure that the EU bodies involved in the fight against cross-border terrorist crimes, such as Eurojust, Europol and – should such decision be taken in the future – the EPPO, receive all necessary resources to fulfil their mandates and carry out their important tasks in protecting the European citizens. The same applies to the Member States in relation to their national authorities.

What may also be envisaged is a narrower and more targeted approach, e.g. a gradual extension of the EPPO's competences, starting with areas that show a strong connection with PIF crimes, such as financial crime in general, organised crime or cybercrime. At a later stage, other types of crime, such as trafficking in human beings, trafficking in arms, and ultimately cross-border terrorist crimes could be included.

---

* The views set out in this article are those of the authors and do not necessarily reflect the official opinion of the European Commission.

1 Cf. the SOTEU 2017 package under https://ec.europa.eu/commission/priorities/state-union-speeches/state-union-2017_en

2 Cf. the Roadmap under https://ec.europa.eu/commission/sites/beta-political/files/roadmap-factsheet-tallinn_en.pdf

3 Cf. the Strategic Agenda 2019–2024 – outline under https://www.consilium.europa.eu/media/39291/en_leaders-agenda-note-on-strategic-agenda-2019-2024-0519.pdf

4 Communication from the Commission to the European Parliament and the European Council – A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes (hereinafter the "Communication"), 12 September 2018, COM(2018) 641 final. See also T. Wahl, eucrim 2/2018, 86–87.

5 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (the 'EPPO'), *O.J. L 283,* 31.10.2017, pp. 1–71.

6 Cf. White Paper on the Future of Europe – Reflections and scenarios for the EU27 by 2025, p. 20 where scenario 3 mentions a "joint public prosecutor's office" to investigate fraud, money laundering and the trafficking of drugs and weapons.

7 This idea was put forward e.g. by Italy's then Minister of Justice Orlando in a letter to Justice Commissioner Jourova and the Estonian Minister of Justice Reinsalu during the Estonian Presidency in the second half of 2017, as well as by French President Macron in his Sorbonne speech on 26 September 2017.

8 Article 120 of the EPPO Regulation foresees that the EPPO assumes its investigative and prosecutorial tasks on a date to be determined by a decision of the Commission on a proposal of the European Chief Prosecutor once the EPPO is set up. As this date cannot be earlier than three years after the entry into force of the EPPO Regulation, the EPPO cannot take up its functions before the end of 2020.

9 Cf. the Communication, *op. cit.* n. 7, p. 1.

10 The following national Parliaments issued an opinion on the Communication: Czech Senate, German Bundestag and Bundesrat, Dutch Tweede Kamer, Romanian Camera dei deputati, and the Swedish Riksdag (to be found on the respective websites of the national Parliaments).

11 Cf. on the EPPO also P. Csonka/A. Juszczak/E. Sason, "The Establishment of the European Public Prosecutor's Office – The Road from Vision to Reality", (2017) *eucrim* , 125–135.

12 The criminal offences falling within the material competence of the EPPO are defined in 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, *O.J.* L 198, 28.7.2017, p. 29. See for this Directive A. Juszczak and E. Sason, "The Directive on the Fight to the Union's Financial Interests by Means of Criminal Law (PIF Directive)", (2017) *eucrim*, 80–87.

13 Cf. Art. 22(2) of the EPPO Regulation and Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, *O.J.* L 300, 11.11.2008, p. 42.

Adam Juszczak

Desk Officer for the EPPO Regulation and the PIF Directive, Directorate General for Justice, Consumers and Gender Equality, European Commission

Elisa Sason

Desk Officer for the EPPO Regulation and the PIF Directive, Directorate General for Justice, Consumers and Gender Equality, European Commission

14 Art. 22(3) of the EPPO Regulation.
15 At the time of adoption of the EPPO Regulation the following 20 Member States participated in the EPPO: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Luxembourg, Portugal, Romania, Slovakia, Slovenia and Spain. On 1 August 2018, the Commission confirmed the Netherlands as the 21st EU Member State (Commission Decision (EU) 2018/1094) and on 7 August 2018, the Commission confirmed Malta as the 22nd EU Member State in the enhanced cooperation (Commission Decision (EU) 2018/1103).
16 EU Member States not participating at this stage are: Denmark, Hungary, Ireland, Poland, Sweden and the United Kingdom. Among those six Member States, Sweden, Poland and Hungary can notify any time their wish to join the EPPO, whereas Ireland and the UK have a special "opt-in" regime (Protocol 21), and Denmark has a special "opt-out" regime (Protocol 22).
17 Cf. for further references https://multimedia.europarl.europa.eu/en/visit-of-stefan-lofven-swedish-prime-minister-ep-plenary_2019043_EP-0878861A_WT5_009_p.
18 Cf. Art. 23 of the EPPO Regulation.
19 It is of note in this context that the EPPO was presented and discussed at the meeting of the Committee of Experts on the Operation of European Conventions on Cooperation in Criminal Matters (PC-OC), Council of Europe on 29 May 2019.
20 Register of Commission Expert Groups and Other Similar Entities, X03578 – EPPO Expert Group pursuant to Art. 20(4) of Council Regulation (EU) 2017/1939.
21 Cf. also Council Decision (EU) 2018/1275 of 18 September 2018 appointing the members of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939, *O.J. L 238,* 21.9.2018, p. 92, *and* Council Implementing Decision (EU) 2018/1696 of 13 July 2018 on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *O.J.* L 282, 12.11.2018, p. 8.
22 Cf. the articles on implementation of the EPPO Regulation in national law by Dubarry/Wachenheim, Herrnfeld, and Villas Alvarez in eucrim 2/2018.
23 Cf. note 21.
24 According to Art. 16 of the EPPO Regulation, the 22 participating Member States shall each nominate three candidates for the post of European Prosecutor.
25 Cf. the Progress Reports towards an effective and genuine Security Union, the most recent of 20.3.2019, COM(2019) 145 final.
26 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, PE/37/2018/REV/1, *O.J.* L 295, 21.11.2018, p. 138–183.
27 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *O.J.* L 135, 24.5.2016, p. 53–114.
28 This draft European Council decision has only two articles. The first article provides for the substantial amendments, while the second merely governs the entry into force. Article 1 of the draft European Council decision reads as follows:
Article 1
Article 86 of the Treaty on the Functioning of the European Union (TFEU) is amended as follows:
"1) In paragraph 1, the first subparagraph is replaced by the following:
'1. In order to combat terrorism and crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust. The Council shall act unanimously after obtaining the consent of the European Parliament.'
2) Paragraph 2 is replaced by the following:
'2. The European Public Prosecutor's Office shall be responsible for investigating, prosecuting and bringing to judgement, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, offences of terrorism affecting more than one Member State and offences against the Union's financial interests, as determined by the regulation provided for in paragraph 1. It shall exercise the functions of prosecutor in the competent courts of the Member States in relation to such offences.'"
29 According to the Commission's proposal for the Regulation on the establishment of the EPPO, COM(2013) 534 final of 17.7.2013, the EPPO was already subject to the review under Protocol No 2. Cf. in this regard the Communication from the Commission to the European Parliament, the Council and the national Parliaments on the review of the proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office with regard to the principle of subsidiarity, in accordance with Protocol No 2, COM(2013) 851 final of 27.11.2013.
30 Cf. Art. 5(3) of the EPPO Regulation.
31 Directive (EU) 2017/541 of 15 March 2017 on combatting terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. In accordance with Art. 28(1) of Directive (EU) 2017/541 Member States were to transpose Directive (EU) 2017/541 by 8 September 2018.
32 Cf. above part II.1.
33 The same applies also to formulating the territorial and personal competence of the EPPO. The Communication acknowledges that these aspects need to be carefully looked into in order to establish the competence of the EPPO for cross-border terrorist crimes.
34 At the same time, in some areas there is a demonstrated need for specialisation through the creation of specialised units within the prosecution office, e.g. in the area of core international crimes.
35 Cf. Art. 37 and the accompanying recital 80 of the EPPO Regulation.
36 Cf. Art. 41 of the EPPO Regulation.
37 Ibid.
38 For overviews of these Directives, see the following articles in eucrim: S. Cras and L. De Matteis, eucrim 4/2010, 153; S. Cras and L. De Matteis, *eucrim* 1/2013, 22; S. Cras, *eucrim* 1/2014, 32; S. Cras and A. Erbežnik, *eucrim* 1/2016, 25; S. Cras, *eucrim* 2/2016, 109; and S. Cras, *eucrim* 1/2017, 35.
39 Cf. in this context also Eurojust Press Release of 21 June 2018 with further references: http://www.eurojust.europa.eu/press/PressReleases/Pages/2018/2018-06-21.aspx. In this Joint Statement a number of Member States call for the creation of a European Judicial Counter-Terrorism Register to be kept at Eurojust.
40 Art. 102 of the EPPO Regulation already provides that the EPPO "may also ask Europol to provide analytical support to a specific investigation conducted by the EPPO", but the instruction power envisaged here would require amending the Europol Regulation as well.
41 Recalling Art. 86 TFEU, which states that the EPPO may be established "from Eurojust".
42 Art. 119(1) of the EPPO Regulation.

Report

The European Crime Prevention Network: Preventing Individual Fraud in the EU

A Report on a New Toolbox

The European Crime Prevention Network (EUCPN) was set up by the Council of the European Union in 2001 (Council Decisions 2001/427/JHA and 2009/902/JHA). For EU Member States, the EUCPN is a first point of contact for crime prevention. The Network collects and disseminates expertise and best practices. The continually evolving thematic focus of the EUCPN reflects the priorities of the EU Policy Cycle, on the one hand, and the EUCPN presidency's priority, on the other. This presidency rotates with that of the Council of the EU.
The EUCPN's output includes toolboxes aimed at local and national practitioners alongside theoretical, research, and policy papers. The toolboxes contain informative studies for practitioners to use, which provide an overview of the problem, present current good practices, and make concrete recommendations for preventive actions. The 13th toolbox in the series published by the EUCPN Secretariat deals with the prevention of individual fraud, after it had been the focal topic of the Bulgarian Presidency in 2018. The following report summarises the main findings on the phenomenon in the EU, best practices, and recommended prevention measures. The full report is available at: <https://eucpn.org/document/toolbox-13-preventing-individual-fraud>.

Individual fraud means that individual citizens are targeted by criminals. Victims are persuaded into a cooperative mindset and defrauded afterwards. Our current understanding of this type of fraud is mainly linked to its contemporary online forms, with phishing as the most common example. However, it is important to realize that individual fraud has been around for ages. The technological developments of the past decades have allowed these scams to be industrialised on a much larger scale than ever deemed possible. Who has not received a phishing e-mail in his or her life?

Victims actively participate in their victimisation. The offender sets his eyes on the victim's money, but he can only gain access to it by persuading the victim to give him access. The essential tactic used to nudge the victim into this compliant relationship is called **social engineering**. It allows the offender to win the victim's confidence, which is crucial to the success of the scam. Social psychology offers us a better understanding of this phenomenon. By appealing to everyday social principles and exploiting "human weaknesses", offenders are capable of activating what is known as the second route of persuasion. The first route requires a great deal of thought and cognitive effort. The second, however, needs no further elaboration and the victim reacts subconsciously. By pretending to be a person in authority, such as a police officer, offenders can easily obtain a level of obedience from their victims. These social and cognitive rules of thumb have their daily uses, but easily allow offenders to exploit them to their own benefit.

Such deceptive tactics are put to use in a wide **variety of scams** (419 scams, granny scams, romance scams, CEO fraud, etc.) – the possibilities are as endless as the creativity of the scammers. This gamut of deceptive schemes allows fraudsters to target a very large public at once or to adopt a more tailored approach. Increasingly, the latter seems to be the case. Scammers have come to realize that by cleverly targeting their victims, their "return on investment" is higher. Phishing emails are becoming more and more sophisticated and addressed to a singled-out target (group). The surprising last step in this trend involves a combination of new and old technology: the telephone. Vishing or voice phishing combines the advantages of both the internet and the telephone. Making an online phone call entails almost no costs, is harder to trace, and can be made automatically. Using the telephone has additional benefits: people trust it and, due to the more intimate setting, victims are persuaded more readily. It is illustrative of the growing level of sophistication that offenders even hire native speakers to make the phone calls in order to seem as genuine as possible.

Our current understanding of individual fraud is limited however. This crime is characterised by a huge **dark number** as so much of it goes unreported. Victims do not know they have even been victimised, they do not perceive the offence as severe enough, they do not believe reporting will lead to anything, or they simply do not know where to report the offence in the first place. In addition, because of the active role, the victim plays in his own victimisation, feelings of self-blame and embarrassment prevent victims from telling their story. Some scams even have "built-in" anti-reporting mechanisms, as the victims have to undertake illegal actions in the scheme, incriminating themselves in the process. Reporting the scam would feel like turning yourself in.

This dark number has also given rise to the **myth** that elderly people are the main victims of this crime, as they are easy prey. Some studies have disproven this myth, although we should remain cautious due to the limited research that is available. Nonetheless, the younger pop-

ulation and middle-aged group are reported to be more susceptible to scams. Another myth that exists is that victims are typically portrayed as uneducated or financially illiterate, but the opposite seems to be true. One possible explanation is called the "knowing-doing gap", where people are successful in recognizing the signs of a scam, but fail to apply this knowledge to their own situation.

Unfortunately, the existence of so-called "**sucker lists**" is not a myth. Phone scammers contact their victims randomly or by looking at public registries, but they also share lists among themselves with targets that already have been defrauded. The use of such lists is indicative of the high level of repeat victimisation. For example, some scammers will even try to "help" you recover your lost assets.

As policing this crime is extremely difficult, the need for prevention is high. However, little academic and evaluative research has been conducted on individual fraud so far. Nonetheless, we can posit some general findings. The most common prevention tactic is educating the public. This can be done in a general awareness raising campaign; there are some positive effects to be noted especially when delivered in some kind of training format. In essence, these trainings try to close the "knowing-doing" gap to which we referred above. Another key tactic is to work with victims. Because of their active role and the existing risk of falling victim multiple times, victims should be supported and be made aware of their vulnerable position.

During the Bulgarian Presidency, the EUCPN Secretariat gathered a number of **good practices** on this topic. These can be categorised according to their target group. A first category focusses on the entire population. Best practices in this context are awareness-raising campaigns, for which we found good examples in Bulgaria, Sweden, Belgium, and from Europol. The campaigns involve radio spots, posters, flyers, gadgets, etc. that provide useful information to the public and show citizens how to protect themselves from being harmed. A second set of activities is targeted towards the elderly. Here, more interactive methods are being employed, e.g., in the Czech Republic. The elderly take part in an interactive educational stage play, where they learn about the most common deception schemes and how to react to them. This "live experience" prepares them to react adequately in real-life situations. An evaluation of this project proved the approach to be empowering, as the active group refused phony deals two and a half times more often than a passive control group that did not participate in the play. The third and last category of prevention activities centres on victims. Examples from Australia, the United Kingdom, and Canada showed the need for this type of prevention on this group. There are, unfortunately, few support services for victims of individual fraud – even globally.

Lastly, the EUCPN report on individual fraud drew up several recommendations on how to prevent phone scams. They are based on a workshop with different experts that was organised by the EUCPN Secretariat in August 2018. These **recommendations** are structured according to the five strategies of situational crime prevention. The first possible strategy is to **increase the effort** an offender must expend in order for the scam to succeed. Restricting the publication of and access to phone numbers can already have a major deterrent effect. Another technique involves limiting the amount of phone numbers one person is allowed to possess or at least to link this "ownership" with a bank account or ID number.

A second strategy is to **increase the risks** for the offender. It is of key importance here to share information. This sharing of information should not stop at the borders of the public or private sectors or even at the national level. All partners have an important part to contribute to the information puzzle. Knowing what you are dealing with increases the chances of preventing it from happening at all. Needless to say, reporting should be made more easy and approachable. Information needs to be gathered before it can be shared. Other recommendations made were to reduce the anonymity of the caller by making it nearly impossible to spoof your location. Voice recognition software could be of interest here.

Reducing the rewards that can be gained by committing this crime is a third strategy to prevent phone scams. Seizing the illegally obtained assets is the main recommendation here. In order to do this, monitoring the flow of money is crucial in detecting suspicious transactions. An EU-wide initiative with the banking sector to facilitate this was recommended by our experts.

Another strategy is to **reduce provocations** that could lead to offending. In this regard, it is import not to share too much information on how the scam was actually executed, as this will prevent copycats. It could also help to prevent some forms of repeat victimisation as some fraudsters will contact identified victims with a deceptive offer to help and retrieve their losses.

The final strategy is to **remove the excuses**. This is mainly focussed on raising awareness on phone scams and how to protect yourself. The good practices mentioned above are key examples. Awareness campaigns should spread the same message. At best, public-private partnerships and international cooperation need to be established in order to spread a consistent message: **just say no.**

Jorne Vanhee
European Crime Prevention Network (EUCPN),
Secretariat – Research officer

Imprint

Impressum

Published by:

Max Planck Society for the Advancement of Science
c/o Max Planck Institute for Foreign and International Criminal Law
represented by Director Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Guenterstalstrasse 73, 79100 Freiburg i.Br./Germany

Tel: +49 (0)761 7081-0
Fax: +49 (0)761 7081-294
E-mail: u.sieber@mpicc.de

Internet: http://www.mpicc.de

Official Registration Number:
VR 13378 Nz (Amtsgericht
Berlin Charlottenburg)
VAT Number: DE 129517720
ISSN: 1862-6947

The publication is co-financed by the European Commission, European Anti-Fraud Office (OLAF), Brussels

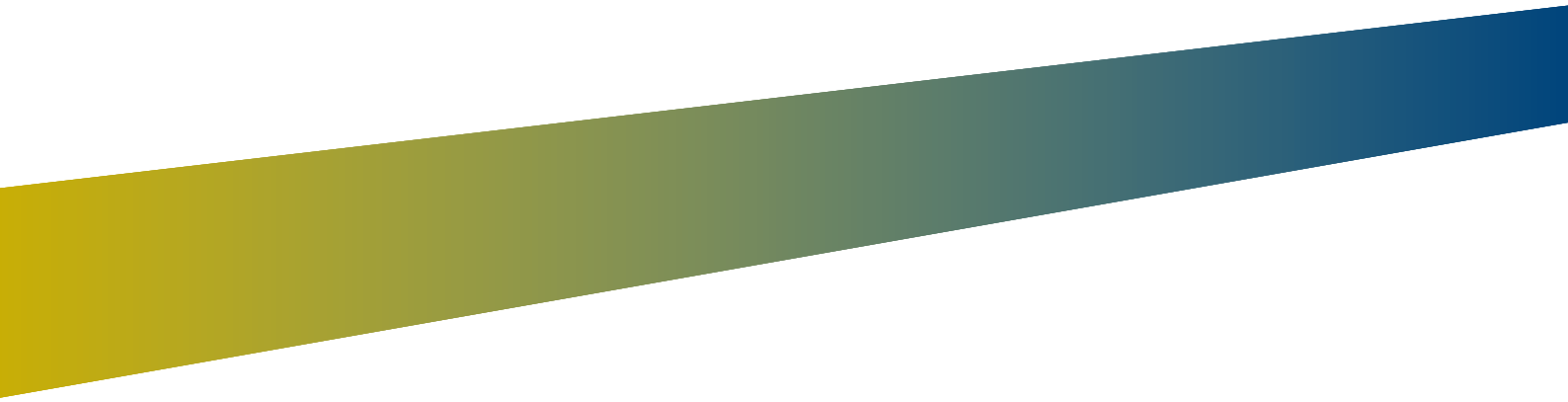
Typeset: Ines Hofmann, Max Planck Institute for Foreign and International Criminal Law, Freiburg
Produced in Cooperation with: Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)
Layout: JUSTMEDIA DESIGN, Cologne
Printed by: Stückle Druck und Verlag, Ettenheim/Germany

Subscription:
eucrim is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@mpicc.de.
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@mpicc.de.

For further information, please contact:

Thomas Wahl
Max Planck Institute for Foreign and International Criminal Law
Guenterstalstrasse 73,
79100 Freiburg i.Br./Germany

Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)
Fax: +49(0)761-7081-294
E-mail: t.wahl@mpicc.de



Max-Planck-Institut
für ausländisches und
internationales Strafrecht