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)