News

Actualités / Kurzmeldungen

European Union*

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

Foundations

Fundamental Rights

Commission Presents New Concept to Strengthen Rule of Law

spot light

On 17 July 2019, the European Commission adopted a set of actions to further strengthen the rule of law in Europe. Key aspects are increased awareness, an annual monitoring cycle, and more effective enforcement. Concrete initiatives are included in the Communication to the European Parliament, the European Council, the Council, the European Social and Economic Committee, and the Committee of the Regions "Strengthening the rule of law within the Union. A blueprint for action" (COM(2019) 343 final). The Communication is linked to a Communication of April 2019 (COM(2019) 163 final, see eucrim 1/2019, p. 3), which set out the existing toolbox to encourage and enforce the rule of law in the EU, inviting all stakeholders to reflect on the next steps. The July Communication takes up the input given during this public consultation. Future avenues will rest on the following three pillars:

- Promotion: Building knowledge and a common rule of law culture;
- Prevention: Cooperation and support to strengthen the rule of law at national level;
- Response: Enforcement at EU level when national mechanisms falter.

When promoting a *rule of law culture*, the Commission will intensify its dialogue with civil society, e.g., by means of an annual event dedicated to rule-of-law principles and by making full use of funding possibilities for civil society and academia in support of their promotion efforts. The Commission is also committed to strengthening cooperation with the Council of Europe (including the Venice Commission and GRECO).

As regards *prevention*, the Commission decided to set up a Rule of Law Review Cycle, including an annual Rule of Law Report summarising the situation in all EU Member States. This is/will be accompanied by a mutual exchange of information and by dialogue, also through a network of national contact persons. The European Parliament and the Council are invited to a dedicated follow-up to the annual Rule of Law Report. The Commission also proposed further developing the EU Justice Scoreboard (see eucrim 1/2019, p. 7), including improved coverage of relevant rule-of-law related areas, such as criminal and administrative justice. In addition, the Commission envisages strengthened dialogue with other EU institutions, Member States, and stakeholders and cooperation with European political parties to ensure that their national members effectively respect the rule of law.

Regarding an effective, common *response* to rule-of-law breaches, the Commission announced that it will continue to make full use of its powers as guardian of the Treaties – it can ensure respect for EU law requirements relating to the rule of law by way of infringement proceedings and the Art. 7 TEU procedure. The Commission will develop and pursue a better strategic approach to infringement proceedings, however, which includes requests for expedited proceedings and interim measures whenever necessary. On Art.7 TEU, the institutions are invited to work together to intensify the collective nature of decision-making among them. The Commission supports the idea of reforming the procedures of the Art. 7 hearing. Building on the Commission Anti-Fraud Strategy (see eucrim 1/2019, p. 15), it will also explore the possibility of a data analysis function to help identify problems when managing risks related to the protection of EU's financial interests.

The Commission established a website which contains all information on

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

the initiative to strengthen the rule of law in the EU. Besides the Communications of April and July 2019, it also includes stakeholder contributions and a summary thereof. According to a recently published Eurobarometer survey on the rule of law, the vast majority of respondents (over 85% in each case) thinks that each of the 17 main principles of the rule of law (e.g., acting on corruption, the independence of judges, the proper investigation of crimes) are essential or important. Over 80% of respondents believes that the situation in their country needs at least some improvement with regard to the respect of these principles. (TW)

Council: Debate on Rule of Law from Justice Perspective

In light of a discussion paper by the Finnish Council Presidency, the Ministers of Justice of the EU Member States held a policy debate on strengthening the rule of law – from the perspective of the justice sector – at their informal meeting in Helsinki on 19 July 2019. Strengthening the rule of law has regularly been on the agenda of the General Affairs Council, but it also has particular importance for judicial cooperation in criminal matters. As Justice Ministers also have a valuable role in strengthening the rule of law, the Finnish Presidency aims to promote regular thematic discussions among Justice Ministers on developments at the EU and national levels, as well as in the case law of the Court of Justice of the EU.

The discussion paper also reflects on the importance of the rule of law for access to justice and sustainable development. It summarises the EU tools supporting a common judicial culture, among them the annual EU Justice Scoreboard (see eucrim 1/2019, p. 7), which is considered "a useful tool for providing comparable information that can support national projects aiming at improving the justice systems." The EU acquis on the procedural rights of suspects and accused persons is highlighted. Against this background, the ministers were invited to discuss, *inter alia*, the following issues:

- Contribution of Justice Ministers to strengthening the rule of law in the EU in the field of justice affairs;
- Regular issues of rule-of-law debates in the JHA Council;
- EU tools considered most effective in supporting a common European judicial culture;
- Further development of EU tools;
- Best practices as regards the rule of law in the field of justice affairs.

Strengthening the rule of law is one of the top priorities of Finland's Council Presidency. The Presidency promotes a comprehensive approach, meaning that the EU's rule-of-law instruments will be regarded as mutually complementary. (TW)

CJEU: Polish Supreme Court Reform Infringes EU Law

On 24 June 2019, the CJEU ruled that the Polish reform lowering the retirement age of the Supreme Court judges is contrary to EU law (Case C-619/18).

The CJEU reviewed the Polish reform law in light of Art. 19(1) subpara. 2 TEU, which obliges Member States to provide remedies sufficient to ensure effective legal protection in the fields covered by Union law. This entails that judges be free from all external intervention or pressure and therefore requires certain guarantees appropriate for protecting those entrusted with the task of adjudicating in a dispute, including the guarantee against removal from office. The principle of irremovability of judges is essential for judicial independence, as required by Union law.

The CJEU rejected the argument brought forth by the Polish government that the reform is intended to standardise the judges' retirement age with the general retirement age applicable to all workers in Poland. The Court points to the explanatory memorandum of the draft law, which casts doubt as to the real aims of said reform. As a result, lowering the retirement age from 67 to 65 for the Supreme Court judges in post was not justified by a legitimate objective and thus undermined the principle of irremovability of judges.

Furthermore, the CJEU held that the conditions and procedures for a potential extension beyond the normal retirement age impair the independence of judges, because the President of the Polish Republic is given unlimited discretion that is not governed by any objective and verifiable criterion.

It is the first final judgment of the CJEU regarding allegations by the EU institutions vis-à-vis EU Member States for not upholding the rule of law. The CJEU's judgment of 24 June 2019 includes fundamental explanations on the Union's principles of the irremovability of judges and of judicial independence. It therefore also serves as a point of reference for discussions on the future strengthening of the EU's rule-of-law monitoring mechanism. This is also one of the priorities of the Finnish Council Presidency in the second half of 2019. The CJEU's decision also influenced the Commission's communication of 17 July 2019 in which it presented a new concept for strengthening the rule of law in the EU. In a statement of 24 June 2019, the Commission highlighted the importance of the judgment.

In the case at issue, the CJEU, by decision of 17 December 2018, already granted interim measures that, *inter alia*, obliged Poland to suspend application of the legislation. A provisional order was issued by the Vice-President of the CJEU on 19 October 2018 in this case. For these decisions, see eucrim 4/2018, p. 191 and 3/2018, p. 144. For the opinion of the Advocate General in the present case C-619/18, see eucrim 1/2019, p. 4. (TW)

AG: Polish Reform Introducing New Retirement Rules for Judges Incompatible with EU Law

On 20 June 2019, Advocate General *Tanchev* presented his opinion on whether the new retirement rules for

Polish judges and prosecutors violate EU law. The case (C-192/18) is an action for failure to fulfil obligations (Art. 258 TFEU), which was brought by the European Commission. The Commission brought forward two complaints against the Polish reform, which introduces new retirement rules in the justice sector:

- The retirement age for judges of common law courts, public prosecutors, and judges of the Supreme Court was lowered to 60 for women and 65 for men, when it was previously 67 for both sexes;
- The Minister of Justice was vested with discretion to prolong the period of active service of individual common law court judges beyond the new retirement ages, when that power was previously exercised by the National Council of the Judiciary.

The AG first concluded that the introduction of different retirement ages for female and male judges is not in line with the EU's secondary law prohibiting discrimination on the grounds of sex. In particular, Poland cannot rely on the discretionary provisions of EU law to set different retirement ages for men and women in public social security schemes.

Second, AG *Tanchev* found that the legislative lowering of the retirement age of judges, together with the discretionary power for the Minister of Justice to extend the active period of judges, does not give the necessary guarantees for judicial independence. In particular, this package is considered to be inconsistent with the objective element of impartiality as protected under the ECtHR case law. Therefore, Poland has also breached its obligations in this regard. (TW)

AG: Poland's New Disciplinary Chamber of the Supreme Court Incompatible with EU Law

On 27 June 2019, Advocate General *Tanchev* delivered his opinion on a reference for a preliminary ruling brought by the Polish Supreme Court (Joined Cases C-585/18, C-624/18 and C-625/18). The referring court casts doubt as to whether the newly created Disciplinary Chamber of the Supreme Court meets the requirements of independence under EU law. The Polish Supreme Court has had to deal with several complaints by Supreme Court judges against their retirement following the new Polish legislation lowering the retirement age of judges.

The case concerns another aspect of the judicial reform in Poland, the Polish legislator having newly created the Disciplinary Chamber of the Supreme Court designated to hear such actions, which were heard prior to the reform before the Chamber of Labour Law and Social Security of the Supreme Court. The Supreme Court questions, however, whether the Disciplinary Chamber offers sufficient guarantees of independence under EU law to hear such claims and whether it can eventually disapply national legislation that transferred jurisdiction to the Disciplinary Chamber. As it stands, the group of judges eligible for appointment by the President of the Republic to the Disciplinary Chamber are selected by the *Krajowa Rada Sądownictwa* (National Council of the Judiciary, 'NCJ') which is the body charged with safeguarding judicial independence in Poland. The independence of the NCJ has been rendered doubtful, however, by Polish legislation modifying the manner in which its judicial members are appointed. Its composition is now primarily determined by the legislative and executive authorities.

In its opinion, AG *Tanchev* first argues that disciplinary regimes governing judges are important aspects of the guarantees of judicial independence under EU law, thus the composition and functioning of a judicial council that itself is not a court must also be assessed in view of the guarantee of judicial independence. The AG admits that there is no uniform model for judicial councils; however, there are common attributes in relation to mission, composition, mandate, and functions that safeguard judicial independence, and the requirements of these attributes must be met under EU law.

After examining the various aspects of the NCJ, the AG concludes that the newly created Disciplinary Chamber does not satisfy the requirement of judicial independence established by EU law. In particular, the manner of appointment of the members of the NCJ compromise its independence from the legislative and executive authorities.

Ultimately, the AG considers that another chamber of a national last-instance court is entitled – of its own initiative – to disapply national provisions that are incompatible with the principle of judicial independence, i.e., in the present case, the law conferring powers to the new disciplinary chamber.

The case is closely connected to other procedures before the CJEU that concern the comprehensive justice reform initiated by the Polish government in 2017. This reform triggered much international criticism and led the Commission to open several infringement procedures against Poland as well as to carry out the so-called Art. 7 TEU procedure by which Poland is put under rule-of-law monitoring. On 24 June 2019, the CJEU held that lowering the retirement age of Supreme Court judges is incompatible with EU law (Case C-619/18). On 20 June 2019, AG Tanchev concluded that the reform of altering the retirement age of judges in lower courts and of prosecutors is in breach of EU law (Case C-192/18). The Commission is conducting further infringement procedures against Poland. (TW)

Commission Advances Infringement Procedure Against New Disciplinary Regime for Polish Judges

On 17 July 2019, the Commission took the next step in the infringement procedure against Poland, eyeing the Polish law that introduced a new disciplinary regime for ordinary court judges. The Commission has now sent a reasoned opinion to Poland after dissatisfaction

with the Polish government's response to a letter of formal notice launched in April 2019.

The Commission is concerned that Poland has introduced the possibility to initiate disciplinary investigations and sanctions against ordinary court judges on the basis of the content of their judicial decisions, including exercise of their right under Art. 267 TFEU to request preliminary rulings from the CJEU. Other critical arguments put forward by the Commission are:

- Due to its composition and selection process, the new Disciplinary Chamber of the Polish Supreme Court is not independent and impartial as required by EU law and CJEU case law;
- The President of Poland's Disciplinary Chamber has such excessive discretionary powers that it is not ensured that a court "established by law" will decide on disciplinary proceedings against ordinary court judges in the first instance;
- It is not guaranteed that disciplinary proceedings against judges are processed within a reasonable timeframe, which undermines the judges' defence rights.

Poland now has two months to react to the arguments of the Commission. If, afterwards, the Commission still considers Poland not to have remedied the complaints, it can bring an action before the CJEU for Poland's failure to fulfil the obligations under EU law.

The question of independence of the Disciplinary Chamber of the Supreme Court is also the subject of a reference for a preliminary ruling (Joined Cases C-585/18, C-624/18 and C-625/18). On 27 June 2019, the Advocate General recommended that the CJEU find incompatibility with EU law in this case, since the Disciplinary Chamber is not sufficiently independent. (TW)

Commission: Rule-of-Law-Related Infringement Actions Against Hungary

On 25 July 2019, the Commission decided to launch an action before the CJEU against Hungary for not fulfilling its obligations under EU law, because Hungary has not changed its so-called "Stop Soros" legislation. The law criminalises activities in support of asylum applications and further restricts the right to request asylum. After having examined Hungary's replies to a reasoned opinion, the Commission found that Hungary has not sufficiently addressed the concerns raised, in particular the incompatibility with the EU's asylum law.

In addition, the Commission filed an action against Hungary at the CJEU for excluding non-EU nationals with long-term resident status from exercising the veterinary profession. This is considered an incorrect implementation of the Long-Term Residents Directive.

In another case, the Commission initiated the infringement procedure by sending a letter of formal notice to Hungary. It criticizes that the detention conditions of returnees in the Hungarian transit zones violate the EU's Return Directive and the Charter of Fundamental Rights of the European Union.

The measures taken by the Commission can be seen in the wider context of the EU's push for Hungary to uphold the value of rule of law. In September 2018, the European Parliament voted to trigger the Art. 7 TEU process, which may ultimately lead to disciplinary sanctions. It was the first time that the Parliament called on the Council of the EU to act against a Member State to prevent a systemic threat to the Union's founding values. (TW)

Fundamental Rights Report 2019

In June 2019, FRA published its fundamental rights Report 2019. The 2019 report places special emphasis on the interrelationship between human rights and the UN's Sustainable Development Goals (SDGs) in an EU context. The 17 SDGs are at the heart of the 2030 Agenda for Sustainable Development, adopted by all United Nations Member States in 2015. They serve as an urgent call for action by all countries in a global partnership to end poverty and other deprivation. This goes hand-in-hand with strategies to improve health and education, reduce inequality, and spur economic growth, while simultaneously tackling climate change and working to preserve oceans and forests.

In the remaining chapters, the report reviews and outlines FRA's opinions on the main developments in 2018:

- Use of the EU Charter of Fundamental Rights;
- Equality and non-discrimination;
- Racism, xenophobia, and related intolerance;
- Roma integration;
- Asylum, borders and migration;
- Information society, privacy, and data protection;
- Rights of the child;
- Access to justice, including the rights of crime victims;
- Implementation of the Convention on the Rights of Persons with Disabilities.

FRA's opinions are available in all EU languages and are additionally compiled in a separate document. They are designed to give advice on possible policy considerations by the EU actors. (CR)

Security Union

19th Progress Report on Security Union

On 24 July 2019, the European Commission presented its 19th "progress report towards an effective and genuine Security Union." The previous report was published on 20 March 2019 (see eucrim 1/2019, pp. 5–6). Within the framework of this series (see also eucrim 3/2016, p. 123), the 19th progress report focuses, in particular, on the following:

- The need for the Union's co-legislators to deliver on pending legislative proposals;
- Enhancement of digital infrastructure security in connection with the fifth generation (5G) networks;
- Analysis of the current risks and vulnerabilities of the EU's anti-money laundering framework (with a package of four reports presented on the same day,

see "Money Laundering" in this issue);
- Areas needing further implementation by the EU Member States;
- Stocktaking of ongoing work to counter disinformation and to protect parliamentary elections against cyber-enabled threats, efforts to enhance preparedness and protection against security threats, and cooperation with international partners on security issues.

The report, *inter alia*, highlights progress made as regards the *prevention of radicalisation online*. Following the "Christchurch call to action" of 15 May 2019, the Commission and Europol initiated the development of an EU crises protocol that will allow governments and Internet platforms to respond rapidly and in a coordinated manner to the dissemination of terrorist content online. The Commission also points out its support of Member States and local actors in preventing and countering radicalisation on the ground in local communities, e.g., the EU-funded Radicalisation Awareness Network (RAN). However, there is an urgent need for the Council and the European Parliament to swiftly conclude the proposed Regulation on preventing the dissemination of terrorist content online (see eucrim 2/2018, pp. 97–98 and the article by *G. Robinson*, eucrim 4/2018, p. 234).

Likewise, the EU co-legislators are called on to reach swift agreement on the legislative proposals for a European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres as well as cross-border access to electronic evidence. Ensuring *cybersecurity* remains one of the key challenges for the EU. Although a lot still needs to be done, the Commission underlines the progress made during the past two years, including – most recently – efforts by the Commission to address sector-specific requirements and recent actions to tackle hybrid threats. In this context, the report also refers to the adopted sanctions regime, which allow the EU to impose targeted, restrictive measures to deter and respond to cyberattacks constituting an external threat to the EU and its Member States.

Another field of EU action is the *strengthening of the EU information systems for security*, border, and migration management. The European Parliament and Council are also called on here to accelerate their efforts in adopting new rules on Eurodac and the Visa Information System as well as the technical amendments necessary to establish the European Travel Information and Authorisation System (ETIAS, see also eucrim 2/2018, pp. 82/84).

A further critical point is the *resilience of digital infrastructure*. In this context, the report refers to the Recommendation on cybersecurity of 5G networks, setting out actions to assess the cybersecurity risks of 5G networks and to strengthen preventive measures (presented in March 2019). As initiated by this Recommendation, Member States completed national risk assessments, on the basis of which a joint review of risks at the EU level will be carried out by October 2019. A common toolbox of mitigating measures is planned for the end of 2019.

As regards the *implementation of other priority files on security*, the report lists a series of legislative acts that have not been fully transposed by the EU Member States; they are called on to take the necessary measures as a matter of urgency. These acts include:
- The EU Passenger Name Record Directive;
- The Directive on combating terrorism;
- The Directive on security of network information systems;
- The 4th Anti-Money Laundering Directive.

The *fight against disinformation* and related interference remains a major challenge for the EU's democratic societies. The EU has put a robust framework in place for coordinated action against disinformation and it took up several measures in the last months. These include:
- The Joint Communication of 14 June 2019 on the implementation of the Action Plan against Disinformation;
- The Rapid Alert System set up in March 2019, which is to facilitate the sharing of insights related to disinformation campaigns and help coordinate appropriate responses;
- The European Cooperation Network on Elections, which held its first meeting on 7 June 2019;
- The envisaged in-depth evaluation of the implementation of commitments undertaken by online platforms and other signatories under the Code of Practice against Disinformation, which was endorsed by the European Council in its conclusions of 21 June 2019.

Ultimately, the report provides updates on the *external dimension* of the EU's security policy. It stresses that leveraging the benefits of multilateral cooperation is an integral part of the EU's efforts towards an effective and genuine Security Union. On 24 April 2019, the EU strengthened cooperation with the UN by signing the framework on counter-terrorism. It identifies areas for UN-EU cooperation and sets priorities until 2020. Several security cooperation measures have also been undertaken with the following partners:
- Western Balkans, e.g., the European Border and Coast Guard Status Agreement between the EU and Albania that entered into force on 1 May 2019;
- Middle Eastern and North African countries with which, for instance, negotiations were launched in view of an international agreement on the exchange of personal data by Europol and the competent national authorities;
- The United States, in relation of which the high-level workshop on battlefield information on 10 July 2019 and the evaluation of the Terrorist Financing Tracking Programme agreement between the EU and the United States (published on 22 July 2019) are highlighted.

In addition, the EU has concluded negotiations on the EU-Canada PNR

Agreement with a view to finalising the Agreement as soon as possible. It will also soon begin joint evaluations of its existing PNR Agreements with Australia and the United States. (TW)

Reflections on Future EU Internal Security

At its meeting on 7 June 2019, the home affairs ministers of the EU Member States began discussing the future of EU policy in the area of internal security, especially law enforcement cooperation. The ministers concurred on the following fields of action:

- Effectively implementating existing legislation, particularly the recently agreed interoperability framework;
- Improving data connection and analysis;
- Pooling resources in research and innovation and building a technology hub;
- Working on a stronger framework for operational cooperation;
- Ensuring a sustainable financial outlook and investing in innovation for internal security, in particular providing Europol with the necessary resources.

The discussion will be continued in more detail during the upcoming Finnish Presidency of the Council. (TW)

Council Calls for New Knowledge-Sharing Platform to Support Law Enforcement

To better connect experts, tools, initiatives, and services in the area of digital data, Europol has been called on to develop a knowledge-sharing platform – the "Novel Actionable Information" (NAI). This is the main outcome of the Council conclusions adopted at the JHA Council meeting on 7 June 2019. The conclusions tackle the problem of the steadily increasing volume of digital data, which have a major impact on criminal investigations by law enforcement authorities. This is why data analysis capacities must be strengthened across Europe and resources, people skills, organisational experience, and services better pooled. Therefore, the EU needs to develop tools that centralise structured knowledge exchange.

The new NAI platform is designed to support Member States and other relevant stakeholders, e.g., agencies, practitioners' networks, etc. in order to:

- Share knowledge on how to conduct (criminal) analysis between law enforcement authorities across the EU;
- Design, update, and use procedures, methodologies, guidelines, manuals, and software programmes on handling digital data;
- Share lessons learned, best practices, and working scenarios involving digital data handling;
- Store applications, algorithms, or other software tools;
- Maintain an overview of relevant initiatives (actions, projects related to knowledge development) to facilitate prioritisation, avoiding duplication and optimising the use of resources.

The NAI platform can include practitioner's competences, e-library capabilities, a toolbox platform, and ongoing or envisaged initiatives.

The Council conclusions also call upon Europol to "set up an Expert Working Group on Criminal Analysis with the objective of aligning standards of criminal analysis." The Member States, agencies, and networks, CEPOL, Eurojust, and the Commission are all called upon to contribute to and support the NAI platform. (TW)

European Preventive Policing: Council Calls for Enhanced Use of Joint Patrols and Joint Operations

In its conclusions on "certain aspects of European preventive policing" of 6 June 2019, the JHA Council invites EU Member States "to make more efficient use of the existing legal framework at national and European level regarding the deployment of officers involved in joint patrols and other joint operations in order to ensure public security in relation to EU nationals on the territory of other Member States."

Member States, EU institutions, and JHA agencies are called on to actively contribute to the implementation of joint patrols and operations. In addition, the Commission should identify suitable financial instruments, and CEPOL should develop targeted training curricula and promote the sharing of best practices in this context. The conclusions also underline "the need for an enhanced, preventive approach to policing methods, striving to contribute to the development of a safer area for all European citizens." (TW)

Security Union: Progress Report on Countering Hybrid Threats

On 29 May 2019, the European Commission and the European External Action Service tabled a report on the EU's progress in tackling hybrid threats.

Hybrid threats are methods or activities that are multidimensional, combine coercive and subversive measures, use both conventional and unconventional tools and tactics, and are coordinated by state or non-state actors. Hybrid threats are characterised by the difficulty in detecting or attributing them to any individual or group. Their aim is to influence different forms of decision-making by a variety of means:

- Influencing information;
- Weakening logistics like energy supply pipelines;
- Economic and trade-related blackmailing;
- Undermining international institutions by rendering rules ineffective;
- Acts of terrorism or to increase (public) insecurity.

The present progress report assesses the implementation of the 2016 Joint Framework on Countering Hybrid Threats – a European Union response and the 2018 Joint Communication Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats. The EU response to hybrid threats is mainly based on 22 countermeasures, ranging from improving information exchange and strengthening the protection of critical infrastructure and cybersecu-

rity to building resilience in the society against radicalisation and extremism.

The report details the progress made in the different areas. It particularly highlights the following advancements:

- Strengthening strategic communications to tackle disinformation;
- Boosting cybersecurity and cyber defence (see also below under "cybercrime");
- Curbing CBRN related risks;
- Protecting critical infrastructure.

Among the key achievements are a large number of legislative measures at the EU level, e.g., the Regulation on the screening of foreign direct investments in the EU and the establishment of autonomous sanctioning regimes against the use of chemical weapons and cyberattacks.

In conclusion, the report highlights enhanced cooperation and coordination as one of the main achievements compared to previous progress reports. This includes not only improved cooperation within and between EU entities – institutions, services and agencies – but also with international partners like the North Atlantic Treaty Organisation and third countries within the framework of multilateral formats, notably the G7. Closer cooperation was also stepped up with partner countries neighbouring the EU.

The report concludes that a "whole-of-society approach" involving government, civil society, and the private sector and including, *inter alia*, media and online platforms is essential for the EU's counter-hybrid policy. (TW).

Countering Hybrid Threats on Agenda of Finnish Council Presidency

Finland, which took up the Council Presidency on 1 July 2019, plans to increase awareness of hybrid threats and to reinforce the EU's common response to them. At the informal meeting of the home affairs ministers of the EU Member States in Helsinki on 18 July 2019, the Finnish Presidency presented a fictious scenario involving hybrid threats and invited the ministers to hold a policy debate about how capacities for the mutual assistance of EU Member States can be strengthened.

Hybrid threats are methods or activities that are multidimensional, combine coercive and subversive measures, use both conventional and unconventional tools and tactics, and are coordinated by state or non-state actors. They include cyberattacks, election interference, and disinformation campaigns. Nowadays, social media platforms are often used for such manipulations.

In a background paper, the Finnish Presidency states that "rapidly evolving hybrid threats are a challenge to security in Europe. They often target wider areas than a single member state and can undermine the unity of the EU."

In this context, Finland would like to strengthen resilience, build up awareness, foster coordination and comprehensive responses across administrative boundaries, and increase cooperation with partners (e.g., the NATO). The goal is also to integrate the various actions and cooperation mechanisms that the EU institutions and the Member States have already started in different policy fields over the last several years. Therefore, further scenario-based debates are planned during the Presidency, involving other policy fields, such as finance, defence, and external relations, besides home affairs. (TW)

Area of Freedom, Security and Justice

Future of EU Substantive Criminal Law

At their meeting on 6 June 2019, the Justice Ministers of the EU Member States debated about a report by the Romanian Council Presidency on the future of EU substantive criminal law. During the Presidency in the first half of 2019, Romania sent a questionnaire to the EU Member States to find out their views on the need to introduce additional harmonising criminal law provisions in new areas within the EU's competence pursuant to Art. 83 TFEU. Issues related to the transposition and implementation of the EU's current regulatory framework were also taken into account.

The Ministers of Justice supported the conclusions of the Presidency Report. They mainly stressed that emphasis should be placed on the effectiveness and quality of implementation of *existing* legislation. They also propounded that further "Lisbonisation" is currently unnecessary, i.e., Framework Decisions that were adopted under the Amsterdam/Nice Treaty should not be transposed and updated by Directives under the Lisbon Treaty. In this context, ministers currently see no need to develop a common definition of certain legal notions, e.g., "serious crime" or "minor offences."

However, the door to the establishment of more minimum rules on criminal offences and sanctions has not yet been completely shut. Instead, the reflection process is to continue. Some Member States and the Commission mentioned *inter alia* the following specific areas where EU legislation would be advisable in the future:

- Environmental crimes, including maritime, soil, and air pollution;
- Trafficking in cultural goods;
- Counterfeiting, falsification, and illegal export of medical products;
- Trafficking in human organs;
- Manipulation of elections;
- Identity theft;
- Unauthorised entry, transit, and residence;
- Crimes relating to artificial intelligence.

In addition, the Presidency report concluded that the EU should improve its dialogue with other international organisations, e.g., the Council of Europe, if the EU envisages legislation in an area that is already covered by an international instrument. The EU should also strive for a high quality of legislation, which is why sufficient time for consultations at the national level should be allotted for. Ultimately, delegations of the EU Mem-

ber States stressed the need for enough time to transpose EU directives, i.e., no less than 24 months. (TW)

Schengen

Group of Schengen States Discusses Challenges for External Land Border Management

At the JHA Council meeting of 7 June 2019, Norway provided information on the joint statement by "the Ministerial Forum for Member States of the Schengen Area with External Land Borders." The Forum met in Kirkenes, Norway on 20–22 May 2019.

The Forum was established and had its first meeting in 2013 at Finland's initiative. It is currently comprised of nine Schengen Member States – Estonia, Latvia, Lithuania, Poland, Norway, Romania, Slovakia, Finland, and Hungary. Ministerial meetings are organised once a year by a different Member State. The aim is to discuss common challenges that the countries are facing as Schengen members responsible for securing and managing the external land border of the entire Schengen area.

The ministers concluded in the joint statement, *inter alia*, that "[f]urther strengthened cooperation among national authorities carrying out tasks related to freedom, security and justice, and between the relevant EU Agencies, is of decisive importance. This will enhance returns, prevention of illegal immigration and cross border crime, improve third country cooperation and will further develop a comprehensive and cost-efficient European Integrated Border Management."

Implementation of the new European Border and Coast Guard regulation will be challenging for the Member States and Frontex, which is why realistic priorities and coordinated timelines must be set. The increased capacities of the European Border and Coast Guard raises challenges for coordination, i.e., the proper balance between use of the capacities at the national level and those required by Frontex.

Common standards for external border surveillance must be developed in an effective and cost-efficient way and in close cooperation between the Member States, the European Commission, and Frontex.

Next year's group ministerial meeting will be held in Romania. (TW)

Legislation

Romanian Presidency: Overview of Legislative JHA Items

On 4 June 2019, the Romanian Council Presidency published an overview of the state of play of legislative proposals in the area of justice and home affairs. Among them:

- The directive on the protection of whistleblowers;
- The multiannual financial framework regarding the Justice Programme and the Rights and Values Programme 2021–2027;
- The "e-evidence package" consisting of the proposed Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the directive on legal representatives for gathering evidence in criminal proceedings;
- Law enforcement access to financial information;
- Removal of terrorist content online.

Eucrim has regularly reported on these matters. (TW)

Institutions

Council

Finnish Presidency Programme

On 1 July 2019, Finland took over the Presidency of the Council of the European Union. In its programme, the Finnish Presidency underlines the need to comprehensively protect the security of EU citizens through, *inter alia*, cooperation in security and defence. The key issues to be addressed are:

- Combating cross-border crime and terrorism;
- Efficient border management;
- Countering hybrid and cyber threats.

Another major issue is the comprehensive management of migration. Some of the measures Finland will strive for during its presidency are:

- Proposals to strengthen the EU's asylum system;
- An EU-wide resettlement system;
- A temporary relocation mechanism for migrants rescued at sea;
- Monitoring of migration routes and maintaining situational awareness;
- Reintegration of returned migrants;
- Strengthening of the European Border and Coast Guard Agency.

The Finnish Presidency is the second in the current trio Presidency after Romania (January – June 2019), followed by Croatia (January – June 2020). (CR)

European Council: Security Remains Priority Area in the Next Five Years

On 20 June 2019, the European Council of the European Union adopted a new strategic agenda for the next five years (2019–2024). Security – which had already been made one of the main priorities by Commission President *Jean-Claude Juncker* during his term of office – remains high on the agenda.

The new agenda focuses on four main priorities:

- Protecting citizens and freedoms;
- Developing a strong and vibrant economic base;
- Building a climate-neutral, green, fair, and social Europe;
- Promoting European interests and values on the global stage.

Regarding the priority area "Protecting citizens and freedoms," the agenda calls to mind that "Europe must be a place where people feel free and safe." In this context, the European Council outlines more specifically political commitments to the following issues:

- Rule of law as a key guarantor for European values; it must be respected by all Member States and the Union;
- Effective control of the EU's external borders;
- Development of a fully functioning comprehensive migration policy, which includes (1) – externally – deepened cooperation with countries of origin and transit in order to fight illegal migration and human trafficking and to ensure effective returns, and (2) – internally – agreement on an effective migration and asylum policy (especially reform of the Dublin regulation);
- Proper functioning of Schengen;
- Strengthened fight against terrorism and cross-border crime, improved cooperation and information sharing, further development of the EU's common instruments;
- Increase in the EU's resilience against both natural and man-made disasters;
- Protection from malicious cyber activities, hybrid threats, and disinformation originating from hostile state and non-state actors; this requires a comprehensive approach with more cooperation, more coordination, more resources, and more technological capacities.

The Strategic Agenda 2019–2024 provides an overall political framework and direction. It is designed to guide the work of the European institutions in the next five years. It will therefore also influence the work of new Commission President *Ursula von der Leyen*. (TW)

European Court of Justice (ECJ)

Judge Egils Levits Resigns

Egils Levits resigned as Judge at the Court of Justice of the EU following his election as President of the Republic of Latvia on 29 May 2019. He had served as Judge at the CJEU since 11 May 2004. (CR)

Death of Advocate General Yves Bot

Advocate General *Yves Bot* passed away on 9 June 2019. He served as Public Prosecutor at the Regional Court of Paris and later as Principal State Prosecutor at the Court of Appeal of Paris. He had been Advocate General at the CJEU since 7 October 2006. Yves Bot was a staunch defender of the values of the European Union and worked throughout his career both to make the justice system more humane and to bring it closer to the people whom it serves. (CR)

OLAF

General Court: No Unlawful Conduct by OLAF vis-à-vis Former European Commissioner

On 6 June 2019, the General Court dismissed the action brought by former Maltese European Commissioner *John Dalli* in which he claimed compensation for non-material damage caused to him by alleged unlawful conduct against him by OLAF and the Commission (case T-399/17).

OLAF opened investigations against Dalli in 2012, alleging him of being involved in an attempt of bribery. Dalli was appointed European Commissioner in 2010 for the portfolio health and consumer protection. It was claimed that Dalli knew about the behaviour of a Maltese entrepreneur who sought to obtain pecuniary advantage from a Swedish tobacco company in return for a more lenient legislative proposal on tobacco products by Dalli's department. The final OLAF report prompted *José Manuel Barroso*, President of the Commission at that time, to urge Mr Dalli to resign from office.

In 2015, the General Court dismissed Dalli's first action in which he sought annulment of the "oral decision of 16 October 2012 of termination of his office" and compensation for damage suffered from that decision (case T-562/12). Dalli addressed the General Court again in 2017 and applied that the Commission be ordered to compensate for the damage, in particular the non-material damage, estimated (on a provisional basis) at €1,000,000.

The Court first rejected the argumentation by the Commission that the present action of 2017 is inadmissible as the matter is *res judicata* following the judgment of 2015. The Court held that the present action has a different cause of action. Whereas the first action related to the decision of the President of the Commission terminating the office of the applicant, the new action mainly related to OLAF's wrongful conduct, which had not actually and necessarily been settled by the first judgment.

As regards the substance of the case, the Court, however, did not find any unlawful conduct on the part of OLAF and the Commission. The Court emphasised that non-contractual liability of the European Union can only be established if the following conditions are fulfilled:
- The unlawfulness of the conduct of which the institutions are accused;
- The fact of damage; and
- The existence of a causal link between that conduct and the damage complained of.

According to case law, the first condition – unlawfulness of the conduct of the institutions – requires a sufficiently serious breach of a rule of law intended to confer rights on individuals to be established. The breach must be one that implies that the institution concerned manifestly and gravely disregarded the limits set on its discretion.

In this context, the Court rejected each of the seven complaints put forward by Mr Dalli concerning the unlawfulness of OLAF's conduct. Those complaints, *inter alia*, concerned the following:
- Unlawfulness of the decision to open an investigation;
- Flaws in the characterisation of the investigation and its unlawful extension;
- Breach of the principles governing the gathering of evidence and distortion and falsification of the evidence;
- Infringement of the rights of the defence, of the principle of presumption of innocence, and of the right to the protection of personal data.

The Court also dismissed two com-

plaints claiming unlawful conduct by the Commission. They concerned:

- Violation of the principle of sound administration and of the duty to behave in a loyal, impartial, and objective manner and to respect the principle of independence;
- Violation of OLAF's independence.

By way of a complementary remark, the Court ultimately held that the applicant did not establish the existence of a sufficiently direct causal link between the conduct complained of and the damage alleged, or even the existence of the latter. Therefore, the third condition of non-contractual liability was not fulfilled either. (TW)

Eurojust & OLAF Increase Cooperation

At a high-level meeting between OLAF and Eurojust on 11 July 2019, both bodies agreed to reinforce cooperation in tackling crimes against the EU budget. Eurojust and OLAF committed to contacting each other at an early stage in order to form joint investigation teams. In addition, the number of coordination meetings between Eurojust national members and OLAF investigators will be increased.

Ladislav Hamran, President of Eurojust, highlighted that Eurojust's and OLAF's mandates are complementary; however, stepping up cooperation is in the interest of both bodies. *Ville Itälä*, Director-General of OLAF, pointed out that the institutional landscape when fighting fraud will change considerably once the European Public Prosecutor's Office starts its operational work. Therefore, adaptations governing the cooperation between OLAF and Eurojust may be necessary.

Currently, the cooperation between OLAF and Eurojust is formally based on an agreement concluded in 2008. (TW)

OLAF and German Prosecutor Trace Misuse of EU Research Money

With the support of OLAF, German authorities (spearheaded by the Mannheim's prosecution service) seized huge amounts of documents and data which are to prove embezzlement and subsidy fraud allegedly committed by four persons between 51 and 56 years of age. They are alleged of having misused several million euros in EU research funds, since they did not pay partners in the research project contrary to contractual obligations.

The prosecution service of Mannheim let the business and private premises of the person concerned be searched in several locations in Germany. On the basis of a mutual legal assistance request and coordination by Eurojust, the French police simultaneously searched premises in the region Provence-Alpes-Côte d'Azur.

The Director-General of OLAF, *Ville Itälä*, commended the teamwork in this joint cooperation. German investigators are currently examining the material. Criminal investigations are ongoing. (TW)

Operation "Postbox II": First Customs-Led Cyber Patrol in Europe

OLAF reported on a significant strike against online criminals trafficking drugs, counterfeit goods, and endangered animal and plant species. Led by OLAF and the Belgian customs service, the operation codenamed "Postbox II" involved customs services from 22 Member States and Europol. It was the first cyber patrol in Europe that was carried out mainly by customs services. The results of the operation were presented by OLAF Director *Ernesto Bianchi* at a press conference at Brussels Airport on 21 May 2019.

The joint customs operation led to 2320 seizures, the opening of 50 case files, and the identification of 30 suspects in Member States. OLAF provided, *inter alia*, assistance by means of its Virtual Operation Coordination Unit, a secure communication system facilitating intelligence exchange in real-time.

Experts raided the cyberspace, i.e., open web, dark net and social media sites, in search of the perpetrators of crime. They used special software and techniques to unveil the sellers' anonymity.

The operation revealed that most counterfeit goods sold had been processed via Asian e-commerce platforms. Drug trafficking mainly takes place through the Dark Web, which allows buyers and sellers top retain their anonymity. (TW)

Action against Illegal and Counterfeit Pesticides

The joint operation "Silver Axe IV" enabled authorities to seize 550 tons of illegal/counterfeit pesticides in 2019. The total amount of this seizure would cover a surface of up to 50,000 km² – approximately equivalent to the territory of Estonia.

The operation involved national police, customs and plant protection authorities from nearly all EU Member States plus Switzerland and the Ukraine as well as private organisations, and other EU bodies, Interpol, and the Food and Agriculture Organization of the United Nations.

OLAF supported the operation by providing information on the movement of smuggled goods. This enabled the identification of suspicious shipments of pesticides (mainly from China) that were not declared correctly. National authorities carried out checks at major seaports, airports, and land borders and in production and repackaging facilities in participating countries.

In the meantime, Operation Silver Axe is in its fourth year. In total, the operations have led to the seizure of 1222 tons of illegal and counterfeit pesticides. (TW)

European Public Prosecutor's Office

Setting up the EPPO – State of Play

The Commission informed the Justice Ministers about the state of play of setting up the European Public Prosecutor's Office (EPPO) at their meeting in Luxembourg on 6 June 2019:

■ Under the Romanian Presidency, the Council adopted Implementing Decision (EU) 2019/598 on the transitional rules for the appointment of European Prosecutors for and during the first mandate period, as provided for in Art. 16(4) of Regulation (EU) 2017/1939. Some European Prosecutors will have a reduced term of office during the first mandate period (three instead of six years). This ensures proper application of the principle of periodical replacement of the European Prosecutors appointed to the EPPO for the first time. According to the Implementing Decision, lots are drawn to select a group comprising one third of the 22 participating Member States – the European Prosecutors in this group will have a reduced mandate. The lots were drawn on 20 May 2019, and the Member States affected are: Austria, Cyprus, Greece, Italy, Lithuania, the Netherlands, Portugal, and Spain.

■ The European Chief Prosecutor has still not been selected and appointed, because negotiations between the European Parliament and the Council came to a deadlock. The Commission calls on the two institutions to quickly resume negotiations after constitution of the new Parliament in order to ensure the timely appointment of the European Chief Prosecutor who plays a key role in setting up the EPPO.

■ Some Member States have not yet submitted their nominations for the position of European Prosecutor.

■ The Commission services prepared a draft for the EPPO's internal rules of procedure. The draft was discussed by the EPPO Expert Group at its meeting on 27–28 May 2019. The internal rules must actually be proposed by the European Chief Prosecutor and, once set up, adopted by the EPPO College by a two-thirds majority (Art. 21(2) Regulation 2017/1939). The Commission stressed, however, that its draft is only a contribution towards facilitating the task of the European Chief Prosecutor and does not prejudice the independence and autonomy of the EPPO.

■ The EPPO's budget for 2019 was adopted and work is ongoing to ensure timely adoption of the draft budget for 2020.

■ As regards the conditions of employment of European Delegated Prosecutors, a preparatory document is currently under discussion.

The Commission is sticking to the timetable that the EPPO can be operational by 2020. However, the swift appointment of the European Chief Prosecutor is essential in order to achieve this aim.

For the Regulation establishing the EPPO under enhanced cooperation, see eucrim 3/2017, pp. 102–104 and the article by *Csonka/Juszczak/Sason* in the same issue on pp. 125–135. (TW)

Europol

Europol 20th Anniversary Website

On 1 July 2019, Europol celebrated its 20th anniversary. On 1 July 1999, German *Jürgen Storbeck*, the former Director of the Europol Drugs Unit (EDU), was appointed as first Europol Director, and Europol commenced its full activities. In view of the 20th anniversary, Europol created a dedicated subpage on its website offering information on its history in an interactive way. It also includes a summary of its twenty most noteworthy operations and a compilation of twenty questions "you always wanted to ask about Europol." While the 20 most noteworthy operations mainly give an overview on Europol's operational development in the last 20 years, the 20 questions give answers to Europol's current operational capabilities and investigative powers. (CR)

Liaison Office Opened in Tirana

On 11 July 2019, Europol officially opened its first liaison office in the Western Balkans, namely in Tirana, Albania. The Europol liaison officer in Tirana will be the counterpart to the Albanian Police liaison officer stationed at Europol's headquarters in The Hague. In order to tackle serious organised crime, the plan is to set up another two Europol liaison offices in the Western Balkans, i.e., in Bosnia and Herzegovina and in Serbia. (CR)

Cooperation with New Zealand

On 11 June 2019, Europol and the New Zealand Police signed a Working Arrangement and Memorandum of Understanding with the aim of strengthening their fight against serious crime, especially online child sexual exploitation, organised motorcycle gangs, drug trafficking, and terrorism. Under the agreement, the New Zealand Police will deploy a permanent liaison officer to Europol's headquarters in The Hague and will be able to use the Secure Information Exchange Network Application (SIENA) managed by Europol. (CR)

Cooperation with NTT Security

On 13 June 2019, Europol and NTT Security signed a Memorandum of Understanding to strengthen their efforts against cybercrime. Under the MoU, parties can exchange threat data and information on cyber security trends and industry best practices. NTT Security is a specialised security company delivering cyber resilience by enabling organizations to build high-performing and effective security, risk and compliance management programmes. (CR)

New Task Force to Combat Migrant Smuggling and Trafficking in Human Beings

On 2 July 2019, Europol launched a new task force to strengthen its fight against criminal networks involved in migrant smuggling and trafficking of human beings. The Joint Liaison Task Force Migrant Smuggling and Trafficking in Human Beings (JLT-MS) will focus on intelligence-led coordinated action with liaison officers from all EU Member States and other partners that are part of this operational platform. It will also support the development of stronger

operational strategies to disrupt international criminal networks. Financial investigations and, ultimately, the gathering of proceeds of crime are expected to become more efficient through the task force. (CR)

Europol Report on Disruptive Technologies and Future Crime

On 18 July 2019, Europol published a report entitled "Do Criminals Dream of Electric Sheep? – How technology shapes the future of crime and law enforcement." The report aims at identifying security threats in relation to new emerging technologies, which can have disruptive effects. The report is also designed to give answers to the challenge of proactive policing and to develop Europol's foresight analysis capacities.

The report looks at key technological developments that are assumed to have a severe impact on the criminal landscape such as Artificial Intelligence (AI), quantum computing, 5G, Dark web networks and cryptocurrencies, the Internet of All Things, 3D printing, molecular biology and genetics. It sets out necessary steps for the law enforcement authorities.

In its conclusions, the report underlines that the opportunities for law enforcement to make use of these technologies are as great as the challenges they pose. Hence, the report stresses the need for law enforcement authorities to invest in understanding these new technologies, to adapt their organisational cultures, to engage with providers, and to take part in scientific discussions. Key factors to maximise effectiveness are seen in resource sharing, joint approaches at national and European level, international cooperation and a robust legal framework. (CR)

Operation OPSON Seizes Fake Food and Drink Products

From December 2018 to April 2019, Europol's Intellectual Property Crime Coordinated Coalition and INTERPOL coordinated Operation OPSON, which resulted in the seizure of some 16,000 tonnes and 33 million litres of potentially dangerous fake food and drink products worth more than €100 million. The operation was supported by police, customs, national food regulatory authorities, and private sector partners from 78 countries. The majority of the seized items consisted of illicit alcohol, cereals and grains, condiments, and even sweets.

OPSON actions were especially targeted at organic food products, 2,4-Dinitrophenol (DNP) – a toxic chemical sold as a fat burner, and fraudulently labelled coffee. (CR)

Operation Against Illicit Fire Arms Trafficking

On 17 July 2018, Europol reported on the Joint Operation "ORION" which was carried out in three operational phases from September 2018 until January 2019. The Joint Operation was conducted by Moldovan and Ukrainian law enforcement agencies, which seized about 300 pieces of small arms, almost 1500 pieces of light weapons, more than 140,000 pieces ammunition and over 200 kg explosives. Furthermore, public awareness campaigns made Moldovan and Ukrainian citizens voluntarily hand over about 2027 light weapons, 54 small arms and 2025 ammunitions with different calibres, as well as 67 pneumatic and gas pistols.

The operation was coordinated by the European Union Border Assistance Mission to Moldova and Ukraine (EUBAM) in cooperation with Europol and supported by the border agencies from Slovakia, Romania and Poland as well as by Frontex and the Southeast European Law Enforcement Center (SELEC). (CR)

Eurojust

New National Member for Finland

On 1 August 2019, Eurojust's new National Member for Finland, *Lilja Limingoja*, took office in The Hague. Ms *Limingoja* had started her career in 1995 as District Prosecutor and since then, has specialized in the area of economic crime. Prior to her appointment as National Member, she has already served as Seconded National Expert at Eurojust, contact point for the European Judicial Network (EJN), and last, as Assistant to the National Member for Finland at Eurojust. (CR)

New Newsletter Available

Eurojust has published its second quarterly newsletter for the year 2019. The newsletter compiles casework highlights for this period, latest publications, key events and other information on Eurojust's support. (CR)

Council Conclusions on Synergies between Eurojust and Judicial EU Networks

At its meeting on 6 June 2019, the JHA Council adopted conclusions "on the synergies between Eurojust and the networks established by the Council in the area of judicial cooperation in criminal matters." The Council acknowledged the vital role played, in the area of cooperation in criminal matters in the European Union, by Eurojust and by four networks established by the Council, namely:

- The European Judicial Network (EJN);
- The Network of Contact Points for persons responsible for genocide, crimes against humanity and war crimes (the Genocide Network);
- The Network of Experts on Joint Investigation Teams (the JITs Network);
- The European Judicial Cybercrime Network (EJCN).

The conclusions mainly endorsed the lines of action proposed in a joint paper by Eurojust and the four networks. The joint paper takes stock of the existing synergies between these networks and between the networks and Eurojust, and it explores areas in which further synergies should be developed. The Council stressed that synergies and coordination

can be further improved in order to combat serious crime and facilitate cooperation in criminal matters more effectively.

Eurojust and the EJN should, in particular, continue efforts to appropriately allocate cases between these two actors in judicial cooperation. The conclusions also acknowledged that Eurojust and the networks must have enough resources at their disposal.

Ultimately, the conclusions support the possibility of establishing a lean secretariat for the EJCN within Eurojust. (TW)

German Prosecutors Call for More Money for Eurojust

On 10 June 2019, the Public Prosecutors General and the Chief Federal Prosecutor of Germany published a resolution expressing their concerns about the European Commission's proposal for the multi-annual financial framework (2021–2027) as far as the funding of Eurojust in this period is concerned. The prosecutors feel that the funding foreseen under the proposal is not efficient enough to allow Eurojust the maintenance of its sound and professional work. The resolution points out that the workload of Eurojust has considerably increased in the last years and will further increase as a result of the operational activities of the European Public Prosecutor's Office in 2020. German public prosecutors relied particularly heavily on Eurojust. In 2018, the number of German cases handled rose by more than 80%. Hence, the Public Prosecutors General and the Chief Federal Prosecutor call on the German Federal Government to plead for an increased funding of Eurojust in the upcoming negotiations on the multi-annual financial framework. (CR)

Eurojust Supports Strike Against Drug Mafia

At the end of July, cooperation among Eurojust, Colombia, the USA, France, Spain and Italy led to the seizure of 369kg of pure cocaine, with a street value of €100 million. Three Italians were arrested, one is suspected of having links to the "Ndrangheta 'Alvaro' di Sinopoli". Due to the support of Eurojust, it was possible to track the drugs throughout their journey from Columbia to Italy through France and Spain. (CR)

Eurojust Supports Strike Against Online Fraudsters

Cooperation between the Irish and Finnish authorities with the support of Eurojust led to a successful strike against an organised crime group (OCG) involved in extended online fraud and money laundering.

Several persons were brought to justice and criminal instruments/assets seized (e.g. fake documentation, equipment for document forgery, laptops and cash). Irish and Finnish authorities agreed at Eurojust on a coordinated investigative and prosecutorial strategy, so that the countries could quickly execute mutual legal assistance requests and collect/exchange evidence in a reliable way. The OCG used fabricated online platforms to offer to unknowing customers non-existent goods exceeding €3 million. (CR)

European Judicial Network (EJN)

52nd Plenary Meeting of the EJN

On 26–28 June 2019, the EJN held its 52nd plenary meeting in Bucharest with the support of the Romanian Council Presidency. The meeting was attended by 135 EJN Contact Points from the EU Member States, candidate, associated and third countries, members of the EJN Romanian Judicial Network in criminal matters, EJN partners, as well as representatives from Eurojust, the European Commission and the General Secretariat of the Council of the EU. The core topics of this plenary meeting were current developments regarding the European Investigation Order, the European Arrest Warrant, and future relations of the EJN with the European Public Prosecutor's Office. (CR)

Frontex

Cooperation Plan with EASO Signed

On 18 July 2019, Frontex and the European Asylum Support Office (EASO) signed an updated Cooperation Plan to further strengthen their cooperation in the fields of asylum, border control and migration management. Under the Cooperation Plan, the Agencies will further work together in the areas of operational and horizontal cooperation, information and analysis, and capacity building. Furthermore, the two bodies will jointly conduct various projects such as the establishment and implementation of the Migration Management Support Teams (MMST), and the delivery of a Common Situational Picture on irregular migration and persons in need of international protection. The Cooperation Plan covers the period from 2019–2021. (CR)

Aerostat Pilot Project Launched

At the end of July 2019, Frontex has launched its aerostat pilot project in cooperation with the Hellenic Coast Guard. The project wants to assess the capacity and cost efficiency of aerostat for operating sea surveillance such as detecting unauthorised border crossings, supporting sea rescue operations and combating cross-border crime. The one-month test period is conducted on the Greek island of Samos. (CR)

Risk Analysis Cell Opened in Dakar

On 12 June 2019, Frontex opened a Risk Analysis Cell in Dakar, Senegal. The cell will collect and analyse strategic data on cross-border crime and support relevant authorities involved in border management. Cells collect information on various types of cross-border crime, e.g. illegal border crossings and document fraud. It is run by local analysts trained by Frontex. The measure is part of the Africa-Frontex Intelligence Community (AFIC) that was launched in 2010 to provide a framework for regular information sharing on migrant smuggling and border security threats. (CR)

Joint Action Plan with Europol Signed

On 7 June 2019, Frontex and Europol signed a new joint Action Plan. The Action Plan foresees a more structured exchange of information between the two agencies, closer coordination in the fields of research into and development of new technologies (e.g., the European Travel Information and Authorisation System (ETIAS)), the exchange of liaison officers, and annual meetings by executive management. (CR)

Liaison Officer Deployed to the Baltic States

At the beginning of May 2019, Frontex' new Liaison Officer to the Baltic States took up his duties. The deployment of liaison officers is part of the creation of a new network of 11 liaison officers to EU Member States and Schengen-associated countries. It enhances cooperation between the agency and the national authorities responsible for border management, returns, and coast guard functions. (CR)

Cooperation with Ukraine Extended

At the end of May 2019, Frontex and the State Border Guard Service of Ukraine extended their cooperation for another three years by signing a new cooperation plan for 2019–2021. Cooperation between Frontex and the State Border Guard Service of Ukraine began in 2007 already, with operational activities, situational awareness, monitoring, and risk analysis as well as joint training. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

Time Limit for Transposing PIF Directive Expired

The EU Member States had to adopt and publish regulations and administrative provisions necessary to comply with Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law (in short: the "PIF Directive") by 6 July 2019. 16 Member States had communicated their implementation measures to the Commission by the transposition deadline, as foreseen in Art. 17(1) of the Directive (10 complete transpositions, 6 partial transpositions). The UK and Denmark are not bound by the Directive.

The Directive, *inter alia*, provides for a common definition of fraud and other criminal offences affecting the EU's financial interests and also for certain types and levels of sanctions when the criminal offences defined in this Directive have been committed. For the Directive, see eucrim 2/2017, pp. 63–64, and the article by *A. Juszczak* and *E. Sason* in the same issue on pp. 80–87.

The Directive is also important for the work of the European Public Prosecutor's Office (EPPO). The catalogue of criminal offences defined in Arts. 3 and 4 of the Directive determines the material competence of the EPPO under Regulation (EU) 2017/1939.

The Directive also applies to VAT fraud if it is considered serious, i.e., when intentional acts or omissions defined in point (d) of Art. 3(2) of the Directive are connected with the territory of two or more Member States of the Union and involve a total damage of at least €10 million. (TW)

ECA Indicates Tax Vulnerabilities of E-Commerce

The EU's and Member States' efforts to collect the correct amount of VAT and customs duties in conjunction with the trade of goods and services via the Internet are not sufficient, as concluded by the Special Report no. 12/2019 by the European Court of Auditors (ECA). The report, which was made public on 12 July 2019, pointed out that e-commerce is growing steadily; however, it is also prone to the evasion of VAT and customs duties. Incorrect levies affect not only the budget of the Member States but also that of the EU, because Member States need to compensate the proportion due to the EU budget.

The audit examined several items in relation to irregularities in the context of e-commerce:

- The system for taxation of VAT and customs duties on cross-border supplies of goods traded over the internet, as set out in the VAT and customs legislation;
- The new system for taxation of VAT on cross-border supplies of e-commerce services that entered into force at the beginning of 2015;
- The new e-commerce legislative reform that was adopted in 2017 and mainly takes effect as of 2021;
- Assessment of whether a sound regulatory and control framework on e-commerce with regard to the collection of VAT and customs duties was put in place by the European Commission;
- Assessment of Member States' control measures intended to help ensure the complete collection of VAT and customs duties in respect of e-commerce.

The ECA acknowledged recent positive developments; however, many challenges have not been satisfactorily addressed to date. Some of the weaknesses are as follows:

- Administrative cooperation instruments in place between EU Member States and with non-EU countries are not being fully exploited;
- The cross-border exchange of information is insufficient;
- Controls carried out by national tax authorities are weak, and the Commission's monitoring activities are insufficient;
- Current customs clearance systems do not function well, and there is a risk that the EU cannot prevent abuse by the intermediaries involved;
- The current system cannot prevent abuse in that goods are deliberately undervalued, so that they do not fall under exemption clauses;
- Enforcement of the collection of VAT and customs duties is ineffective.

In order to address these shortcomings, the ECA's report makes a number

of recommendations to the Commission and the Member States. Notably, they have been asked to do the following:

- Check traders' compliance thresholds for VAT/customs;
- Develop a method to produce estimates of the VAT gap, i.e., the difference between what should be collected in accordance with the current legislative framework and what is actually collected by Member States' tax authorities;
- Explore the use of suitable "technology-based" collection systems to tackle VAT fraud involving e-commerce.

Fortunately, the ECA found that some of the identified weaknesses can be solved by the new e-commerce reform, e.g., the liability of VAT intermediaries. However, some challenges remain, e.g., the problem of undervalued goods.

The ECA special report also includes the Commission's response to the findings. It is available in 23 EU languages. (TW)

ECA: Fighting Fraud in the Cohesion Sector is Unsatisfactory

Member States made improvements in identifying fraud risks and in designing preventive measures, but detection, response, and coordination efforts must be considerably strengthened when it comes to tackling fraud in cohesion spending.

This is the main conclusion drawn by the European Court of Auditor's (ECA) Special Report no. 06/2019. Although the Commission and Member States share the responsibility to counter fraud and any other illegal activities affecting the EU's financial interests, in the field of EU cohesion policy, the managing authorities in the Member States are primarily responsible for setting up proportionate and effective anti-fraud measures. It is especially apparent that incidences of reported fraud are significantly higher in EU cohesion spending compared to other areas of EU spending: around 40% of reported fraud cases and almost three quarters of the total amount (€1.5 billion) of irregularities relate to EU cohesion policy. Cohesion policy includes the European Regional Development Fund, the Cohesion Fund, and the European Social Fund.

Against this background, the ECA carried out an audit assessing whether managing authorities have properly met their responsibilities at each stage of the anti-fraud management process: fraud prevention, fraud detection, and fraud response.

The ECA found that managing authorities have improved their fraud risk assessment as regards cohesion funding for the 2014–2020 programming period. However, the ECA detected a number of flaws:

- Some Member States' analyses were not sufficiently thorough, and Member States generally have no specific anti-fraud policy;
- No significant progress towards proactive fraud detection and use of data analytics tools;
- Procedures for monitoring and evaluating the impact of prevention and detection measures often insufficiently monitored;
- As regards fraud response, managing authorities, in coordination with other anti-fraud bodies, not sufficiently responsive to all detected cases of fraud;
- Limited deterrent effect of correction measures;
- Insufficient coordination of anti-fraud activities;
- Suspicions of fraud not systematically communicated to investigation or prosecution bodies;
- Fraud cases underreported, affecting the reliability of figures in Commission PIF reports.

The ECA made a number of recommendations as a result of the audit. They are addressed to the Member States, the Commission, and the EU legislator. Member States are called upon to do the following:

- Develop formal strategies and policies to combat fraud against EU funds;
- Involve external actors in the process of fraud risk assessments;
- Improve the use of data analytics tools.

The Commission should monitor fraud response mechanisms in order to ensure consistency and encourage Member States to expand the functions of their Anti-Fraud Coordination Services (AFCOS).

For cohesion spending in the period 2021–2027, the Union legislator should make compulsory the adoption of national strategies or anti-fraud policies and the use of proper data analytics tools. Furthermore, it should introduce sanctions and penalties for those responsible for fraud against the EU's financial interests. Ultimately the EU should lay down minimum rules for AFCOS to ensure effective coordination.

For the 2021–2027 programme, the ECA also made recommendations for more performance-orientated cohesion spending in a Briefing Paper issued on 20 June 2019.

The Special Report is available in 23 EU languages. It also contains a response by the Commission to the findings of the ECA. (TW)

Tax Evasion

New Data Mining Tool to Combat VAT Fraud

Since mid-May 2019, EU Member States are able to use a new electronic tool that is expected to detect VAT fraud at an early stage. The Transaction Network Analysis (TNA) is an automated data mining tool that interconnects Member States' tax IT platforms. In this way, cross-border transaction information can be quickly and easily accessed, and suspicious VAT fraud can be reported nearly in real time.

Besides closer cooperation between the EU's network of anti-fraud experts ("Eurofisc"), when analysing information on carousel VAT fraud, TNA also boosts cooperation and information exchange between national tax officials. Eurofisc officials can now cross-check

information against criminal records, databases, and information held by Europol and OLAF.

TNA is another EU tool to make the collection of VAT more fraudproof. In the midterm, the Commission hopes to reach consensus on a more fundamental overhaul of the EU's VAT legislation (see eucrim 4/2017, pp. 168–169). (TW)

Money Laundering

Commission: Better Implementation of the EU's AML Framework Needed

spot light

On 24 July 2019, the Commission published a Communication and four reports that assess the risks of money laundering and the implementation of the EU's anti-money laundering/countering terrorist financing (AML/CFT) framework. The package is designed to support European and national bodies so that they may better counter the risks of money laundering. It also contributes to the debate on potential future policy measures to further strengthen the EU' AML/CFT rules.

The Communication summarises the development of the legal framework to date and gives an overview of the four reports:

- Supranational Risk Assessment Report;
- Report assessing recent alleged money laundering cases involving EU credit institutions;
- Report assessing the framework for cooperation between Financial Intelligence Units;
- Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts.

The four reports are analysed in more detail in separate news items.

In general, the Commission concludes that the EU has established a solid AML/CFT regulatory framework; however, divergencies in the application of the framework were clearly revealed by the reports. The Union must make an effort to avoid fragmentation and failures in the application of the legislation.

In this context, the full implementation of the fourth and fifth AML Directives is indispensable. A number of structural problems in the Union's capacities to prevent AML/CFT must be addressed.

The Commission puts forward three main issues for policy discussions:

- Further harmonisation of the AML/CFT rulebook by transforming the AML Directive into a Regulation, thus creating directly applicable Union-wide rules;
- Conferral of specific anti-money laundering supervisory tasks to a Union body in order to achieve the aim of high-quality and consistent supervision of the financial sector;
- Establishment of a stronger mechanism to coordinate and support cross-border cooperation of and analysis by Financial Intelligence Units.

As a result, the Communication and the reports of 24 July 2019 outline policy options that may be taken up by the new incoming Commission under *Ursula von der Leyen*. (TW)

2019 Risk Assessment Report on Money Laundering

The Supranational Risk Assessment (SNRA) report of 24 July 2019 systematically analyses the money laundering or terrorist financing risks of specific products and services. It focuses on vulnerabilities identified at the EU level, both in terms of legal framework and in terms of effective application, and provides recommendations for addressing them. The report is published biannually as required by Art. 6 of the 4th AML Directive. The 2019 SNRA updates the first SNRA report published on 26 June 2017 (see eucrim 2/2017, pp. 65–66) and follows up on recommendations made to actors involved in the fight against money laundering/terrorist financing.

The SNRA assesses the risks in various sectors, e.g. cash/cash-like assets, the financial and gambling sector, and the collection and transfers of funds through non-profit organisations. Compared to the 2017 report, the 2019 report identified additional products and services that are potentially vulnerable to money laundering and terrorist financing, including privately owned automated teller machines (ATMs), professional football, free ports, and investor citizenship and residence schemes ("golden passports/visas").

The report found that most recommendations of the first report have been implemented by the various actors; however, several horizontal vulnerabilities common to all sectors were identified. The major snags are:

- Anonymity in financial transactions, which is particularly the case for some e-money products, virtual currencies, and unregulated crowdfunding platforms;
- Difficulties with identification of and access to beneficial ownership information;
- Weaknesses in supervision within the internal market in terms of controls, guidance, and the level of reporting by legal professionals;
- Gaps in cooperation between Financial Intelligence Units (see also FIU report).

The 2019 SNRA also makes a number of recommendations that are addressed to the European Supervisory Authorities, non-financial supervisors, and the Member States. Sector-specific recommendations are included. The Commission will follow up these recommendations in the next report in 2021. (TW)

Commission Brings AML Regulation Into Play

spot light

On 24 July 2019, the Commission published a report on recent alleged money laundering cases involving EU credit institutions (COM(2019) 373 final). This report is the Commission's response to requests from the European Parliament and the Council to carry out a thorough review of whether there are structural flaws in the regulatory and supervisory frame-

work – against the background of a number of recent money laundering incidents involving European banks.

The report analyses possible shortcomings in relation to the credit institutions' AML/CFT defence systems and the reaction of public authorities to the events. As regards credit institutions, the report identified four broad categories into which shortcomings may be grouped:

- Ineffective or lack of compliance with the legal requirements for anti-money laundering/countering the financing of terrorism systems and controls;
- Governance failures in relation to anti-money laundering/countering the financing of terrorism;
- Misalignments between risk appetite and risk management;
- Negligence of anti-money laundering/countering the financing of terrorism group policies.

The analysis of the reactions of bank institutions led to the following main results:

- Substantial failures to comply with core requirements of the Anti-Money Laundering Directive, such as risk assessment, customer due diligence, and reporting of suspicious transactions/ activities to FIUs;
- AML/CFT compliance deficiencies;
- Risky businesses pursued without establishing commensurate controls and risk management;
- Lack of consistent compliance and control process policies.

On the positive side, thanks to the gradual development of the AML/CFT legal framework in the past several years, many of the credit institutions reviewed have taken substantial measures to improve their compliance systems.

As regards the public side, the report found that supervisory reaction varied greatly in terms of timing, intensity, and measures taken. Major factors that hampered an effective reaction include:

- Attribution of different degrees of priority and resource allocation to AML-/CFT-related activities; often, supervision was not carried out frequently enough;
- Sometimes, lack of relevant experience and available tools;
- Too much focus on the AML framework of the host Member State, without paying requisite attention to cross-border dimensions, particularly when bank groups were supervised;
- The division of responsibilities led to ineffective cooperation between anti-money laundering authorities, prudential authorities, Financial Intelligence Units, and law enforcement authorities;
- Cooperation with third-country AML/CFT authorities and enforcement authorities proved difficult in some cases.

Notwithstanding, the report stresses that several improvements were made, especially during the last two years. They include targeted amendments of the relevant legal framework, particularly with respect to the prudential framework and enforcement through the European Banking Authority. Many authorities have been or are being reorganised and are acquiring additional resources and new expertise.

The Commission concludes that some of the shortcomings have been or will shortly be addressed by changes in the regulatory framework. Many structural problems remain, however, and the EU needs to address them. These problems are mainly based on regulatory and supervisory fragmentation in the AML/CFT area. Therefore, the Commission recommends the following:

- Appropriately attributing the tasks of the various relevant authorities involved in the fight against money laundering and terrorist financing;
- Cooperating with key third countries in a more structure and systematic way, ensuring concerted positions in said cooperation;
- Considering further harmonisation of the AML/CFT rules, in particular turning the AML Directive into a Regulation that would create directly applicable rules in the entire Union;
- Conferring specific anti-money laundering supervisory tasks to a Union body in order to ensure high-quality and consistent anti-money laundering supervision, seamless information exchange, and optimal cooperation between all relevant authorities in the Union.

The incoming Commission is expected to take up these rather long-term options and enhance future discussions with the relevant stakeholders and political institutions. (TW)

Commission: Need for Reinforced FIU Cooperation

In a series of anti-money laundering reports (all published on 24 July 2019), the Commission assessed the framework for cooperation between Financial Intelligence Units (FIUs), as required, for instance, by Art. 65(2) of the 5th AML Directive.

FIUs were established under the EU's AML/CFT legal framework; their main tasks are regulated by the AML Directive 2015/849. FIUs are central national units in each Member State. They act independently and autonomously. Their main tasks are to receive and analyse suspicious transaction reports and information relevant in the fight against money laundering, associated predicate offences, and the financing of terrorism. They disseminate the results of their analysis and any other information to the competent national authorities and to other FIUs. At the EU level, FIUs cooperate via their own platform, an informal expert group composed of representatives from the Member States' FIUs and FIU.Net, an information system connecting decentralised databases enabling FIUs to exchange information. The FIUs are considered to be a central player in the EU's AML/CFT framework, positioned between the private sector and competent law enforcement authorities (police, prosecutors, courts).

The different types of cooperation in relation to FIUs were the subject of the assessment, i.e.:

- Cooperation between FIUs and with reporting entities;
- Cooperation between FIUs in the

EU, including exchange of information, matching of data sets, joint analyses, and FIU.Net;
- Cooperation between FIUs and supervisors;
- Cooperation of FIUs with third countries.

The Commission concludes that cooperation has improved greatly over the past few years. However, several shortcomings remain, e.g.:
- Remaining uneven status of FIUs in Member States, which affects their ability to access/share relevant financial, administrative, and law-enforcement information;
- Lack of regular feedback by FIUs to the private sector on the quality of their reports and lack of a structured dialogue between them in order to share typologies/trends and give general guidance;
- Lack of a common approach when dealing with threats common to all Member States;
- Development of more efficient IT tools; common tools based on artificial intelligence and machine learning are needed;
- Technical difficulties in the functioning of FIU.Net, which are one reason for the continued insufficient cooperation between the Member States' FIUs;
- Slow dissemination of information;
- Limited scope of the FIUs' Platform, e.g., it cannot produce legally binding templates.

The Commission also notes that some elements were addressed by the most recent Directive 2019/1153, adopted on 20 June 2019, on access to financial and other information. The Directive does not solve all issues, however, since it does not, for instance, include rules on precise deadlines and IT channels for the exchange of information between FIUs from different Member States. Moreover, the scope of the Directive has been limited to cases of terrorism and organised crime associated with terrorism, as a result of which it does not cover other forms of serious crime (contrary to the initial proposal by the Commission).

Ultimately, the Commission suggests some concrete changes, such as a new support mechanism for cross-border cooperation and analysis. The EU finally needs to think about building up more centralised structures. (TW)

Commission Prepares Interconnection of Central Bank Account Registries

In parallel with other reports in the area of anti-money laundering, on 24 July 2019, the Commission published a report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts (COM(2019) 372 final).

The report relates to Art. 32a of the 5th AML Directive (Directive (EU) 2018/843 amending Directive (EU) 2015/849), which obliges Member States to put in place national centralised automated mechanisms by 10 September 2020. These mechanisms should enable the identification of any natural or legal persons holding or controlling payment accounts, bank accounts, and safe deposit boxes. The Directive also lays down the minimum set of information that should be accessible and searchable through the centralised mechanisms; Financial Intelligence Units (FIUs) should have immediate and unfiltered access to them, while other competent authorities should be granted access in order to fulfil their tasks/obligations under the AML Directive. Directive 2019/1153 on facilitating access to financial and other information further obliges Member States to designate the national authorities competent for the prevention, detection, investigation, and prosecution of criminal offences; they should have direct, immediate, and unfiltered access to the minimum set of information of such centralised mechanisms. At the least, these competent authorities should include the Asset Recovery Offices.

The present report helps build up the interconnection of the centralised automated mechanism, as required by Art. 32a (5) of the 5th AML Directive. It looks at the various IT solutions ensuring the EU-wide, decentralised interconnection of national electronic databases (already existing or currently under development). The available technical options are analysed and benefits and drawbacks explored.

As regards future steps, the Commission concludes that the envisaged system could possibly be a decentralised system with a common platform at EU level. Already developed technology could be used. The Commission intends to further consult with the relevant stakeholders, governments, as well as the FIUs, law enforcement authorities, and Asset Recovery Offices as potential "end-users" of such a potential interconnection system. To this end, the Commission must prepare a legislative proposal for the establishment of the interconnection. (TW)

New Directive on Law Enforcement Access to Financial Information

spot light

The European Parliament and the Council adopted new legislation that improves the access of law enforcement authorities to financial information. Directive (EU) 2019/1153 "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" was published in the Official Journal L 186 of 11 July 2019, p. 122. The Commission initiated the Directive in April 2018 (for the proposal, see eucrim 1/2018, pp. 13–14).

While the EU has built up a robust anti-money laundering framework (providing for several obligations on the part of private entities), rules to date do not set out the precise conditions under which national authorities can use financial information for the prevention, detection, investigation or prosecution of certain criminal offences. In particular, the EU wants to give national authorities direct access to bank account information contained in national centralised

bank account registries, which all Member States must set up under the 4th and 5th AML Directives.

Against this background, the Directive pursues several aims:

- To facilitate access to and the use of financial information and bank account information by competent law enforcement authorities, including Asset Recovery Offices and anti-corruption authorities;
- To facilitate access to law enforcement information by Financial Intelligence Units (FIUs) for the prevention and combating of money laundering, associate predicate offences, and terrorist financing;
- To facilitate cooperation between FIUs;
- To ensure information exchange with Europol.

As a result, the new Directive entails the following obligations for the EU Member States:

- To designate which competent authorities can have direct and immediate access to bank account information for the prevention, detection, investigation or prosecution of certain criminal offences, and which authorities can request information or analysis from the FIUs;
- To ensure that FIUs are required to cooperate with the competent authorities and are able to reply to requests for financial information or analysis from those authorities in a timely manner;
- To ensure that the designated competent authorities reply to requests for law enforcement information from the national FIU in a timely manner;
- To ensure that FIUs from different Member States are entitled to exchange information in exceptional and urgent cases related to terrorism or organised crime associated with terrorism;
- To ensure that the competent authorities and the FIUs are entitled to reply (either directly or through the Europol national unit) to duly justified requests related to bank account and financial information made by Europol.

Beyond the EU's general data protection framework (in particular, Directive 2015/680), the Directive provides for specific and additional safeguards and conditions for ensuring the protection of personal data, e.g., as regards the processing of sensitive personal data and the records of information requests.

EU Member States must now implement the Directive into their national laws by 1 August 2021. (TW)

Counterfeiting & Piracy

Commission: Directive on Protecting the Euro by Criminal Law Must Be Transposed More Efficiently

The Commission is not fully satisfied as to how Member States have transposed Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law. In a report published on 9 May 2019 (COM(2019) 311), the Commission concluded: "the majority of the Directive's provisions have been transposed by the majority of the Member States. However, almost all Member States have transposition issues with one or several provisions, […]"

The Directive updates a previous Framework Decision on the same subject by introducing a reinforced system on the level of sanctions, investigative tools, and the analysis, identification, and detection of counterfeit euro notes and coins during judicial proceedings.

Examples for recurrent flaws in the transposition of the Directive are:

- Some Member States established separate categories of minor/petty/or non-aggravated forms of the offences defined under Arts. 3 and 4 of the Directive, where penalties remained below the level required by the Directive (see the provision on minimum/maximum sanctions in Art. 5 of the Directive);
- Many Member States did not transpose Art. 8(2) lit. b), which requires the establishment of jurisdiction over offences committed outside the territory of the Member States whose currency is the euro and on the territory of which the counterfeit euro or coins have been detected;
- A large majority of Member States did not adequately transpose Art. 10 of the Directive on the transmission of seized counterfeit currency to the National Analysis Centre (NAC)/Coin National Analysis Centre (CNAC);
- The provision on statistics (Art. 11) has not been transposed by almost all Member States.

In conclusion, the Commission report stresses that there is currently no need to revise the Directive, but Member States must take the appropriate measures to ensure full conformity with the provisions of Directive 2014/62. If necessary, the Commission will launch infringement proceedings. (TW)

Intellectual Property Crime Threat Assessment

spot light

For the first time, Europol and the European Union Intellectual Property Office published a joint EU-wide intellectual property (IP) crime threat assessment analysing the emerging threats and impact of IP crime in the EU. It focuses on counterfeiting and piracy affecting the EU.

One of the key concerns outlined in the report is the growing discrepancy between the increasing number of counterfeit and pirated goods in overall world trade and the decreasing number of seizures of counterfeit items by customs authorities in the EU. The report concludes that this development is influenced by the fact that IP crime is not a top law enforcement priority, as it is often perceived as a victimless crime. At the EU level, counterfeiting was also removed as a priority from the EU Policy Cycle on Serious and Organised Crime 2017–2021.

In addition, counterfeiters no longer produce only fake luxury items but deal in a wide range of everyday goods, e.g., car parts, cosmetics, electronic components, food and drink, toys, etc. According to the report, today any product with

a name brand can become a counterfeiting target, with significant consequences for both the economy and the health and safety of consumers.

Key product sectors for piracy are electronics, food and drink, luxury products, clothes and accessories, pesticides, pharmaceuticals, tobacco products, and vehicle parts, with China being the main source of counterfeit items for almost every type of counterfeit good. Another catalyst in the growth of counterfeit goods is the continued growth of e-commerce and global distribution possibilities offered by online marketplaces and social media marketplaces, which facilitate the trade of counterfeit items.

As regards the perpetrators, the report outlines that most criminal activity involving counterfeiting is performed by organised criminal groups that are usually also involved in other criminal activities. Lastly, the report also notes a (still very small) growing production of counterfeit goods in the EU. (CR)

Cybercrime

Report on Cybercrime Challenges

Eurojust and Europol published a joint report on common challenges when combating cybercrime. The challenges are analysed from two perspectives: law enforcement and the judicial.

The report analyses five main areas:

- Loss of data;
- Loss of location;
- Challenges associated with national legal frameworks;
- Obstacles to international cooperation;
- Challenges of public-private partnerships.

For each of these areas, the report also discusses ongoing activities and open issues.

Open issues identified in the report with regard to *loss of data* include, for instance, the need for a new legislative framework regulating data retention for law enforcement purposes at the EU level. Furthermore, law enforcement no longer has access to non-public information from WHOIS (a database of registration and contact information on the owners of domain names) due to a new GDPR compliance model. Other open issues are the need to identify solutions for crypto-currency investigations and to provide law enforcement with adequate tools, techniques, and expertise in order to counter the criminal abuse of encryption.

With regard to *loss of location*, the report emphasises the need for an international legal framework for direct cross-border access to data. In order to overcome the *challenges associated with national legal frameworks*, the report recommends developing an EU-wide legal framework within which to conduct online investigations, specifically in the Deep Web and Dark Web. To improve *international cooperation*, the international legal framework should be rounded out to allow for consistent and efficient cross-border cooperation.

Finally, legislative measures to improve *public-private partnerships* are needed to facilitate cooperation with private partners and to balance privacy-related needs with the need to support law enforcement in the fight against cybercrime. The report also calls for clear and transparent rules on the involvement of private parties in the gathering of evidence. (CR)

Cybersecurity Act Introduces Cybersecurity Certification and Strengthens EU's Cybersecurity Agency

On 7 June 2019, the EU added another piece of cybersecurity legislation: the "Cybersecurity Act" (= Regulation (EU) 2019/881); it was published in the Official Journal L 151, p. 15. It introduces a framework for European Cybersecurity Certificates and reinforces the mandate of the EU Agency for Cybersecurity (ENISA). The Regulation had been proposed by the Commission as part of the "cybersecurity package" following the State of the Union Address by Commission President *Jean-Claude Juncker* in 2017 (see eucrim 3/2017, pp. 110–111).

It is clarified that this Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security, and the activities of the State in areas of criminal law.

The EU *Cybersecurity Certification Framework* is an internal market measure that lays down the main horizontal requirements for the development of European cybersecurity certification schemes. The mechanism attests that ICT products, ICT services, and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of, e.g., protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data.

Several advantages are expected from the new certification framework:

- Citizens/end users: increase in trust in digital products, because they can be sure that everyday devices/services are cyber-secure;
- Vendors and providers of products/services (including SMEs and start-ups): first, cost and time savings, because they must undergo the certification process only once, and the certificate is valid throughout the entire EU; second, the label can be used to make products/services more attractive for buyers/users, as they are labelled "cyber secure";
- Governments: better equipped to make informed purchase decisions.

Certification schemes established under the new EU framework are voluntary, i.e., vendors/providers can themselves decide whether they want their products/services to be certified. The Cybersecurity Act foresees, however, that the Commission will assess the mechanism and reflect on whether specific European cybersecurity certification schemes should become mandatory.

The Cybersecurity Act changes ENISA's mandate from a temporary one into a permanent one. ENISA will also

receive more staff and money in order to fulfil its tasks. Current tasks, such as supporting policy development and the implementation of cybersecurity acts (e.g., the NIS Directive) and capacity building will be strengthened. New tasks have been added; ENISA will play a key role in implementing the Union's policy on cybersecurity certification. ENISA will also play a greater role in promoting cooperation and coordination on matters related to cybersecurity. Ultimately, it will be an independent centre of expertise on cybersecurity. (TW)

New Sanctioning Regime Against External Cyber-Attacks

The Council has established a framework that allows the EU to impose restrictive sanctions against external cyber-attacks threatening the Union or its Member States. The framework consists of:

- Council Regulation (EU) 2019, 796 (which is based on Art. 215 TFEU);
- Council Decision (CFSP) 2019, 797 (which is based on Art. 29 TEU).

The acts were published in the Official Journal L 129 I, 17.5.2019, 1. They entered into force on 18 May 2019.

The framework comes in response to recent malicious cyberattacks that originated or were carried out outside the EU and affected the EU Member States' critical infrastructure, competitiveness, and/or state functions. It is a measure within the EU's Common Foreign and Security Policy (CFSP) and part of the "cyber diplomacy toolbox."

The framework applies to cyber-attacks with a "significant effect," including attempted cyber-attacks with a potentially significant effect. Cyber-attacks that constitute an external threat to the Union or its Member States include those which:

- Originate, or are carried out, from outside the Union;
- Use infrastructure outside the Union;
- Are carried out by any natural or legal person, entity, or body established or operating outside the Union;
- Are carried out with the support, at the direction of, or under the control of any natural or legal person, entity, or body operating outside the Union.

The Regulation allows the Council to list natural or legal persons, entities or bodies who/which are responsible for such cyber-attacks, who/which provide financial, technical or material support, or who/which are associated with the responsible or supporting persons. Targeted sanctions against these listed persons include:

- Entry ban into or transit ban through the EU;
- Freezing of all funds and economic resources;
- Prohibition of EU citizens and entities from making funds available to those persons listed.

According to the recitals of the Decision, the new sanctioning regime may also be applied in case of cyber attacks with a significant effect against third countries or international organisations if this is necessary to achieve CFSP objectives.

It is also clarified, that the targeted restrictive measures must be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State. (TW)

No More Ransom Initiative Turns Three

On 26 July 2019, the No More Ransom initiative celebrated its third anniversary. Today, the portal offers decryption to 109 different types of ransomware infections and is available in 35 languages. 150 partners, consisting of 42 law enforcement agencies, 5 EU Agencies and 101 public and private entities, have joined the initiative since its start in July 2016 (see eucrim 3/2016, p. 128). (CR)

Law Enforcement Cracks Down on GrandGrab

On 17 June 2019, several European and international law enforcement agencies, together with Europol, released a decryption tool for the latest version of the most prolific ransomware family GrandCrab. With the tool, victims of ransomware can regain access to the electronic files encrypted by hackers on their computers or mobile devices without having to pay a ransom. The tool is available free of charge on www.nomoreransom.org. (CR)

Terrorism

EU Terrorism Situation and Trend Report 2019

Europol published the EU Terrorism Situation and Trend Report 2019 (TE-SAT 2019). It outlines the latest developments with regard to jihadist terrorism, ethno-nationalist and separatist terrorism, left-wing and anarchist terrorism, right-wing terrorism, and single-issue terrorism.

Looking at jihadist terrorism, key observations from the year 2018 indicate that all fatalities from terrorism in 2018 were the results of jihadist attacks committed by terrorist acting alone and targeted at civilians as well as symbols of authority. The number of fatalities dropped from 62 people in 2017 to 13 in 2018. While completed jihadist attacks were carried out using firearms and unsophisticated, readily available weapons, several disrupted terrorist plots included the attempted production and use of explosives and chemical/biological materials. A general increase in chemical, biological, radiological and nuclear (CBRN) terrorist propaganda, tutorials, and threats was also observed. Although activities by the Islamic State (IS) decreased in 2018, IS still intends to carry out attacks outside of conflict zones. Both IS and al-Qaida keep up a strong online presence, seeking new multipliers for their propaganda. Still, no terror-

ist group demonstrated the capacity to carry out effective cyberattacks in 2018. The number of European foreign terrorist fighters travelling, or attempting to travel, to the Iraqi and Syrian conflict zones, was very low in 2018 but a shift in focus can be seen towards carrying out attacks in the EU. In addition, the number of returnees to the EU remained very low in 2018. According to the report, there seems to be no systematic abuse of migration flows by terrorists entering the EU. In particular, minors returning to the EU are at the heart of Member States' concerns, as these persons are victims, on the one hand, but have been exposed to indoctrination and training, on the other.

Looking at ethno-nationalist and separatist terrorism, the report reveals that these attacks greatly outnumber other types of terrorist attacks in 2018. Although the number of attacks linked to left-wing and right-wing terrorism was still relatively low, the number of arrests linked to right-wing terrorism continued to markedly increase. Terrorism financing is still intensively being conducted via the Hawala banking instrument (transfer or remittance of values from one party to another, without use of a formal financial institution such as a bank or money exchange).

In total, 129 foiled, failed, and completed attacks were reported by EU Member States in 2018, with the highest number of attacks having been experienced by the UK (60). 1056 individuals were arrested in the EU on suspicion of terrorism-related offences, with the highest number of arrests in France (310). 17 EU Member States reported convicting or acquitting 653 persons of terrorist offences in 2018, the average prison sentence being seven years. (CR)

Judicial Counter-Terrorism Register at Eurojust

During the annual meeting on counter-terrorism at Eurojust from 20 to 21 June 2019, national experts agreed on further practical steps to implement a judicial counter-terrorism register. The register will centralise judicial information on counter-terrorism proceedings from all EU Member States. It establishes links between judicial proceedings against suspects of terrorist offences and helps Eurojust offer better coordination.

The register was initiated by France, Germany, Spain, Belgium, Italy, Luxembourg and the Netherlands following the terrorist attacks in Paris and Saint-Denis in November 2015. They showed the need for the judicial authorities to get a quick overview of judicial proceedings in other EU Member States against terrorists who increasingly operate across borders.

The Counter-Terrorism Register (CTR) focuses on judicial proceedings and convictions only, and therefore will not overlap with the criminal analysis carried out by Europol. The new EU database does not include only jihadist terrorism, but also terrorist offences from extreme right and left-wing groups in Europe. The CTR was launched on 1 September 2019. (CR)

New Reporting Series Kicked Off with ECTC Report on Women in IS Propaganda

In mid-June 2019, Europol published its first report in a new series called "Europol Specialist Reporting" – a collection of reports on priority crime areas published by Europol's in-house experts.

The first report, published by Europol's European Counter Terrorism Centre, looks at women in Islamic State (IS) propaganda. It analyses how the IS appeals to women, the doctrinal dialectics put forward by IS with regard to women, their expected role(s) in jihad, and how the organisation uses Islamic jurisprudence to mould the role of women within jihad.

Its key findings include a noticeable increase in women featured in IS propaganda as well as a broader scope in the nature and extent of their roles within the organisation. Nevertheless, the preferred nature of women remains that of the traditional stay-at-home mother and wife. According to the report, the motivation of female jihadists is similar to that of their male counterparts: they are driven by the wish to join a cause and to contribute to building an Islamic state.

Remarkably, the report finds IS propaganda to be filled with disparaging and condescending descriptions of women. This, however, seems to be perceived differently by women who subscribe to IS ideology, as their roles are seen as unnegotiable and emanating from a divinely authoritative source. (CR)

Evaluation of the EU-US Agreement on Tracing Terrorist Financing

On 22 July 2019, the Commission presented the "joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program." It is the fifth evaluation report on the agreement which entered into force on 1 August 2010.

The agreement enables law enforcement authorities to get timely, accurate, and reliable information about activities associated with suspected acts of terrorist planning and financing. It helps identify and track terrorists and their support networks worldwide.

The EU and USA agreed on regular joint reviews of the safeguards, controls, and reciprocity provisions to be conducted by review teams from the European Union and the USA (Art. 13 of the Agreement). The fifth evaluation report covers the period from 1 January 2016 to 30 November 2018. It is limited to the description of procedural aspects and a summary of the recommendations and conclusions. A more detailed Commission staff working document accompanies the report.

In general, the Commission is satisfied that the Agreement and its safeguards and controls (e.g., data protection) are being properly implemented. During

the evaluated period, over 70,000 leads were generated, some of which brought forward investigations into terrorist attacks on EU territory, such as those in Stockholm, Barcelona, and Turku. The number of leads increased considerably compared to almost 9000 in the previous reporting period (1 March 2014 to 31 December 2015). EU Member States and Europol are increasingly using the mechanism.

The report also includes a number of recommendations for further improvement, *inter alia*:

- Better cooperation between EU Member States' authorities and U.S. counterparts with regard to the necessity of retaining so-called "extracted data";
- Regular feedback from Member States to Europol on the added value of leads received from the U.S. authorities;
- Continuation of Europol's efforts to raise awareness of the TFTP and to support Member States seeking advice and experience when making requests;
- Improved verification by the U.S. Treasury with respect to data protection rights.

The next joint review will be carried out at the beginning of 2021. (TW)

Council Conclusions on Radicalisation in Prisons

At its meeting on 7 June 2019, the home affairs ministers/ministers of the interior of the EU Member States adopted Council conclusions on preventing and combatting radicalisation in prisons and on dealing with terrorist and violent extremist offenders after release. The Council pointed out that effective measures in this area must urgently be taken, because of the growing number of terrorist offenders and offenders radicalised in prison and because a number of them will be released in the next two years.

The conclusions were based on Member States' responses to a questionnaire on policies for the prevention and countering of radicalisation in prisons, discussions at the working level of the Council, and Member States' written comments. Member States have been, *inter alia*, invited to further develop specialised interventions for dealing with terrorist and violent extremist offenders as well as with offenders assessed as in risk of being radicalised while serving time in prison.

The Commission has, in particular, been invited to support several activities in the Member States, such as the development of tools and practices for risk management, the implementation of training programmes for relevant professionals and practitioners (prison staff, probation officers, the judiciary, etc.), de-radicalisation, disengagement and rehabilitation programmes for terrorist and violent extremist offenders, etc. Support may also include the work of third countries and partners, especially neighbouring regions, such as the Western Balkans, the MENA-region (Middle East and North Africa), and the Sahel in order to prevent radicalisation in prisons.

Good practices on addressing radicalisation in prisons and dealing with terrorist and violent extremist offenders after release have been annexed to the conclusions. Good practices include, for instance:

- Swift information exchange among relevant stakeholders and development of dedicated strategies;
- Setting up of specialised and multidisciplinary units responsible for countering violent extremism and radicalisation in prisons;
- Comprehensive training programmes for prison and probation staff;
- Implementation, if necessary, of special measures for individuals convicted of terrorist offences, based on a risk assessment;
- Measures encouraging inmates to disengage from violent extremist activities on a case-by-case basis and support for religious representatives to provide alternative narratives;
- Education, training, and psychological support after release as well as further monitoring of radicalised individuals who are considered to pose a continued threat. (TW)

Illegal Employment

Workers' Perspective on Severe Labour Exploitation

In June 2019, FRA published its fourth report on the topic of severe labour exploitation, focusing on the perspective of the workers. The report is based on interviews with 237 exploited workers. It outlines the following:

- Pathways into severe labour exploitation;
- Working and living conditions of employees;
- Employers' strategies to keep the workers working;
- The interviewees' perception of risk factors for severe labour exploitation;
- Employees' access to justice.

In its conclusions, the report recommends acting on recruitment, i.e., by setting minimum EU standards for employment and recruitment agencies and their subcontractors. Another suggestion is to enforce the legal framework for labour law, i.e., by reinforcing workplace inspections with the support of the planned European Labour Authority and by the adoption of the EU Directive on transparent and predictable working conditions. Another key issue is to inform workers of their rights and the existence of labour exploitation. Migrants should avoid irregular residence status, as it strengthens the employers' position of power.

In this context, the report asks EU Member States to increase legal avenues for migration and to create targeted labour migration programmes. The power of employers is also strengthened by policies that tie the residence permit to the existence of an employment contract. Residence permits and visas should give migrants the possibility to quickly switch employers. Residence status also permits many victims of la-

bour exploitation to report to the police. Therefore, the report sees the need to shift the authorities' focus from immigration enforcement to the protection of workers and labour rights. Lastly, the report recommends taking measures to develop a culture of rights among relevant stakeholders in the labour market as well as among the general population. (CR)

Procedural Criminal Law

Procedural Safeguards

All Procedural Rights Directives Now Apply

The transposition period for the directive on special safeguards for children in criminal proceedings (Directive 2016/800) ended on 11 June 2019. Together with the directive guaranteeing access to legal aid (Directive 2016/1919), which had to be transposed by 25 May 2019, it is the last piece of legislation that had to be implemented according to the 2009 Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings.

The acts complement the other rights that already apply, i.e.:

- The right to be presumed innocent and to be present at trial (Directive 2016/343);
- The right of access to a lawyer (Directive 2013/48);
- The right to information (Directive 2012/13);
- The right to interpretation and translation (Directive 2010/64).

The Commission advised the Member States to implement the recent Directives as soon as possible if they have not done so yet. The Commission provides support through workshops or expert meetings.

For an introduction to the various Directives, see the contributions of *Steven Cras* (partly with co-authors), all available at the eucrim website. (TW)

CJEU: Italian Law Differentiating Applicability of Negotiated Settlements in Line with EU Law

In its judgement of 13 June 2019 in case C-646/17 (criminal proceedings against *Gianluca Moro*), the CJEU followed the conclusions of Advocate General (AG) *Bobek* of 5 February 2019 (for the AG's opinion, see eucrim 1/2019, pp. 24–25). It confirmed that the following legal situation is in line with the provisions of Directive 2012/13 on the right to information in criminal proceedings and Art. 48(2) CFR: under Italian law, an accused can apply for a negotiated penalty – known as *patteggiamento* – after the start of the trial if the facts of the criminal charge are modified, but not if the charge is legally reclassified.

The CJEU first rejected the position of the Italian government that the request for a preliminary ruling is inadmissible, because Directive 2012/13 is only applicable if there is a cross-border element in the main proceedings. Like the AG, the CJEU argued that the Directive contains minimum rules for criminal procedures in also purely domestic cases that do not have a cross-border constellation.

As regards the material question, the CJEU focused on the interpretation of Art. 6(4) of Directive 2012/13, 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 CJEU, the Directive stipulates how the right to fair trial can be guaranteed as far as the information of the suspect or accused person is concerned. This right encompasses the obligation to inform the accused person if the charge has been modified, be the modification of a factual or a legal nature. The accused person must be in a position to effectively react to a possible change in the nature of the accusation. By contrast, the Directive does not entail any legal obligation to guarantee the accused person's right to apply for a negotiated penalty during the trial.

Art. 48 CFR does not change this result. Its guarantee to respect the rights of the defence of anyone who has been charged does not include any obligation that goes beyond what already exists in Directive 2012/13.

In sum, Union law does not preclude domestic procedural rules that 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 a factual nature and not when the change is of a legal nature. (TW)

Fair Trials: Study on Threats to Presumption of Innocence Regarding Presentation of Suspects in Criminal Proceedings

On 3 June 2019, Fair Trials – a NGO that stands for improving respect for a fair trial in accordance with international standards – released a report on key threats to the presumption of innocence if suspects are presented in public environment. The report focuses on:

- Prejudicial statements by public authorities;
- Press coverage;
- Presentations in courtroom and public settings.

The report is based on the evaluation of a wealth of data, i.e.:

- Global survey of law and practice on the presentation of suspects;
- Sociological study on the impact of images of arrest and different measures of restraint on public perceptions of guilt;
- Content analysis of crime-related news stories in newspapers, the online press, and broadcast television news programmes in seven countries;
- Comparative research on the presentation of suspects before the courts in five countries (Hungary, France, Croatia, Malta, and Spain).

The report does not make a comparative analysis by presenting reports on a country-by-country basis but by exploring key issues and themes as well as useful examples of good practice from the provided data.

Fair Trials makes a number of recommendations on how compliance with the international standards on the presumption of innocence can be improved in the situations studied. As an overall recommendation, the report states:

"a. The EU Directive [2016/343] is an important first step in making the presumption of innocence a reality in Europe but the EU will have to invest considerable time and political will to ensure its effective implementation. Member States' courts will also have to refer questions to the CJEU where it is unclear what EU law requires.

b. Meaningful reform will require profound changes of law, practice and culture. Robust laws are important, but a formalistic legal approach will not suffice. Long-term engagement of law enforcement, legal professionals (including judges, prosecutors and the defence) and the media will be crucial, alongside broader public education."

The report also annexes a checklist for journalists reporting on criminal suspects; it was developed by the University of Vienna. (TW)

Data Protection

Works on Interoperability of EU Information Systems Can Start – Legal Framework Established

spot light

On 22 May 2019, the new rules establishing a framework for interoperability between EU information systems in the field of borders and visa (Regulation (EU) 2019/817) and in the field of police and judicial cooperation, asylum and migration (Regulation (EU) 2019/818) were published in the Official Journal of the European Union (O.J. L 135). The Regulations that had been initiated by the Commission on 12 December 2017 (see eucrim 4/2017, pp. 174–175) were adopted by the Council on 14 May 2019. After publication in the Official Journal, the Regulations entered into force on 11 June 2019. The various interoperability components need technical implementation, however, which is why the date of the operational start of the components is determined by the Commission. It is expected that they can be applied by 2023.

The two sets of Regulations had become necessary, because the legal bases of the information systems were different and the levels of EU Member States' involvement in the various databases varied. Nonetheless, both Regulations largely contain identical provisions.

The interoperability framework solves the problem that, to date, data are separately stored in various large-scale IT systems at the EU level, but the systems can principally not communicate with each other. This may lead to information gaps, e.g., information could get lost or criminals with several or false identities may remain undetected. The Regulations therefore pursue several different objectives (defined in Art. 2(1) of the Regulations):

- Improve effectiveness and efficiency of border checks at external borders;
- Contribute to prevention and combating of illegal immigration;
- Contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States;
- Improve implementation of the common visa policy;
- Assist in examination of applications for international protection;
- Contribute to prevention, detection, and investigation of terrorist offences and other serious criminal offences;
- Facilitate identification of unknown persons who are unable to identify themselves or unidentified human remains in cases of a natural disaster, accident, or terrorist attack.

Hence, the interoperability framework focuses on the correct identification of persons and on combating identity fraud. At the same time, it will, *inter alia*, improve data quality and harmonise the quality requirements for data stored in EU information systems (cf. Art. 2(2)).

In order to achieve the objectives, the Regulations establish the following interoperability components and specify their purposes, use, queries, access possibilities, etc.:

- European search portal (ESP): it enables the competent authorities of the Member States and the Union agencies to gain "fast, seamless, efficient, systematic and controlled access" to the EU information systems, to Europol data, and to Interpol databases. The ESP can be used to search data related to persons or their travel documents. The ESP does not change the access rights of the authorities/Union agencies. After having launched a query to the ESP (by submitting biographic or biometric data), the system indicates which EU information system or database the data belongs to. The ESP will not provide information regarding data in EU information systems, Europol data, and Interpol databases that the user has no access to under applicable Union and national law.
- Shared biometric matching service (shared BMS): it is a technological tool to match the individual's biometric data across different systems; it will regroup and store all biometric templates in one single location that are currently being separately used in the EU information systems. In this way, it will enable the searching and comparing of biometric data (fingerprints and facial images) from several systems;
- Common identity repository (CIR): it contains biographical and biometric data of third-country nationals available in several EU information systems. It aims to increase the accuracy of identification through automated comparison and matching of data.
- Multiple-identity detector (MID): it checks whether the biographical identity data contained in the search exist in other systems covered in order to enable the detection of multiple identities linked to the same set of biometric data.

An infographic provided for at the

Council website illustrates how the tools work.

The Regulations apply to the following EU information systems:

- The Entry/Exit System (EES);
- The Visa Information System (VIS);
- The European Travel Information and Authorisation System (ETIAS);
- Eurodac;
- The Schengen Information System (SIS);
- The European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

Regulation 2019/818 also applies to Europol data to the extent of enabling them to be queried simultaneously alongside the EU information systems referred to. As regards personal scope, the Regulations apply to persons whose personal data may be processed in the EU information systems referred to and/or in the Europol database.

In order to mitigate interference into the rights and freedoms of the persons concerned, the Regulations include several safeguards, e.g.:

- Full access to data contained in the EU information systems that is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond access to identity data or travel document data held in the CIR, will continue to be governed by the applicable legal instruments;
- Authorised end-users cannot make adverse decisions for the individual concerned solely on the basis of the simple occurrence of a match-flag;
- Provisions regulate the log-keeping of queries, the obligations to (principally) inform individuals whether links to their person have been established, penalties for misuse of data, and liability;
- A web portal will be established for the purpose of facilitating the exercise of the rights of access to, rectification, erasure, and restriction of processing of personal data.

The web portal will be developed by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). The Agency will also be responsible for the development of the interoperability components, the technical management of the central infrastructure of the interoperability components, data quality standards, etc.

The establishment of interoperability was hotly debated in the runup to the legal framework. In particular, data protection experts took a critical stance (see eucrim 1/2019, pp. 26–27). Despite this criticism and before the adopted legal framework becomes operational, Statewatch has reported that the EU is already thinking of making customs information systems interoperable with EU Information Systems in Justice and Home Affairs, e.g., the SIS. The working groups at the EU level will further explore the potential added value of cross-checking relevant goods and persons' data between customs and JHA databases. (TW)

Infringement Proceedings for Not Having Transposed EU Data Protection Directive

On 25 July 2019, the Commission lodged an infringement action against Greece and Spain before the CJEU for having failed to transpose Directive 2016/680 regarding the protection of personal data by law enforcement authorities (for the Directive, see eucrim 2/2016, p. 78). The deadline for transposing the rules of the Directive into national law ended on 6 May 2018. The Commission also called on the CJEU to impose financial sanctions in the form of a lump sum against the two countries in accordance with Art. 260(3) TFEU.

The Commission stressed that failure to transpose the directive leads not only to problems in the exchange of law enforcement information but also to an unequal treatment of persons as regards the protection of their fundamental rights. To date, Greece and Spain have not notified their laws, regulations, and administrative measures that would comply with Directive 2016/680, as a result of which the two countries breached their obligations under EU law.

On the same day, the Commission started an infringement procedure against Germany for not having completely transposed Directive 2016/680. The Commission observed that only 10 of the 16 federal states (*Länder*) had adopted measures implementing the Data Protection Law Enforcement Directive by the end of the transposition period on 6 May 2018. The Commission sent a letter of formal notice to Germany, which is the first step in the infringement procedure. Germany now has two months to reply to the arguments raised by the Commission. Otherwise, the Commission may decide to send a reasoned opinion, i.e., to start the second phase of the infringement procedure.

Directive 2016/680 was part of the EU data protection reform along with the General Data Protection Regulation (GDPR). It pursues a twofold aim: better protection of the individual's personal data processed by law enforcement authorities in the EU Member States (both in purely domestic processing as well as in the cross-border exchanges of data); at the same time, a more efficient and effective exchange of data due to the harmonisation. The directive replaces Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters with effect from 6 May 2018. (TW)

Implementation of the GDPR: Commission Generally Satisfied

Over a year after the application of the General Data Protection Regulation (GDPR), the European Commission makes an overall positive assessment. In a report, published on 24 July 2019, the Commission concludes that most Member States have set up the necessary legal framework and that the new governance system is falling into place. Individuals increasingly make use of their rights, and businesses are developing a compli-

ance culture. EU data protection rules are increasingly being used as a point of reference at the international level. The report also includes a number of issues that need to be further improved, e.g.:

- Ensuring that all Member States comply with EU data protection rules;
- Strengthening the role of data protection authorities;
- Supporting and involving stakeholders from civil society and business;
- Making sure that individuals and businesses, including SMEs, can enjoy the benefits brought about by the GDPR;
- Integrating data protection into all relevant policies;
- Further promoting international convergence towards a high level of data protection rules.

The GDPR has been applicable since 25 May 2018. Their rules are directly applicable in all EU Member States. It does not apply, however, to the processing of personal data for national security activities or law enforcement. For the latter, Directive 2016/680 forms the legal basis for data processings.

The national Data Protection Authorities are in charge of enforcing the new rules and are better coordinating their actions through new cooperation mechanisms and the European Data Protection Board. They are issuing guidelines on key aspects of the GDPR in order to support the implementation of the new rules in the private and public sectors.

The Commission will report on the progress made in the implementation of the GDPR in 2020 again. (TW)

Draft Data Protection Guidelines on Video Surveillance

On 10 July 2019, the European Data Protection Board (EDPB) published draft guidelines on processing of personal data through video devices. The aim of the guidelines is to ensure the correct, consistent application of the EU's General Data Protection Regulation (GDPR) in cases of video surveillance. The guidelines cover both traditional video devices and smart video devices. They were subjected to a public consultation.

The guidelines first clarify the scope of application. In this context, the GDPR does not apply to processing of data that has no reference to a person, e.g., in cases involving fake cameras, and also not to the processing of data by the competent authorities for law enforcement purposes (where the data protection Directive 2016/680 applies).

Other items addressed by the guidelines include:

- Lawfulness of processing;
- Disclosure of video footage to third parties;
- Rights of the data subject;
- Transparency and information obligations;
- Storage periods and obligations to erasure;
- Technical and organizational measures.

The guidelines may be further refined after the public consultation which ended on 9 September 2019. Guidelines for other GDPR-related areas will follow. (TW)

Reference for Preliminary Ruling on Data Protection and Judicial Independence

The Administrative Court of Wiesbaden, Germany referred two questions for a preliminary ruling to the CJEU that deal with Regulation 2016/679 – the General Data Protection Regulation (GDPR) – and the independence of the judiciary in the federal state of Hesse. The reference by the administrative court of Wiesbaden is registered as case C-272/19 at the CJEU. The full text of the reference (in German) is available at OpenJur.

In the case at issue, the complainant sought information about his personal data, which is stored at the Petitions Committee of the Hesse Land Parliament. The president of the parliament rejected the claim, arguing that the petition process is a parliamentary task exempt from the rights of data subjects as established by the federal state's data protection law implementing the European data protection regulation.

The administrative court doubts that this exclusion is in conformity with the EU's GDPR. It believes that the Petitions Committee functions as a public authority, which is why a natural person has also the right to access to information in accordance with Art. 15 and Art. 4 No. 7 GDPR.

In addition, the administrative court poses a more fundamental question: is the court actually allowed to make references to the CJEU, because it may not be an independent and impartial tribunal as required by Art. 267 TFEU read in conjunction with Art. 47(2) of the Charter of Fundamental Rights of the European Union. In essence, the referring court argues that the German legal order only establishes the independence of judges, whereas the "court" as institution is "conducted" by the justice ministry of the federal state. The ministry manages personnel files, is responsible for recruiting the judges, and participates in lawsuits among applicants or judges.

Put in focus: The second question, on the independence of German judges, is surprising. However, it interpolates with the general debate in Germany as to the extent to which institutions of the judiciary are really independent in the sense of international and European standards. It relates to the recent CJEU judgment that declared German public prosecution services not having sufficient independence to issue European Arrest Warrants (see eucrim 1/2019, pp. 31–33). If the CJEU follows the argumentation of the German court, it will have to make fundamental reflections on the admissibility of references for preliminary rulings by German courts. (TW)

PNR Collection also for Maritime and Railway Traffic?

The Finnish Council Presidency intensifies discussion on whether the scope of the EU's Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation, and

prosecution of terrorist offences and serious crime (Directive (EU) 2016/681) should be broadened. In a discussion paper, tabled on 25 June 2019, the Finnish Presidency invites the other Member States to discuss the usefulness and benefits of gathering PNR on other travelling forms.

The EU Directive (see eucrim 2/2016, p. 78) only applies to air carriers operating extra-EU flights; Member States can, however, decide to apply the same obligation to intra-EU flights, which most Member States do. PNR data may contain different types of information, such as travel dates, travel itinerary, ticket information, contact details, means of payment used, seat number, and baggage information. Law enforcement authorities consider the data useful for investigating and preventing crime.

The discussion paper points out that the travel volume inside and outside the Schengen area are both increasing. All forms of cross-border travelling pose risks to security, e.g., migrant smuggling, drug smuggling, terrorism, etc. Therefore, uniform EU rules on the use of PNR data on other forms of transportation, such as sea traffic and international high-speed trains, may offer added value. In this context, the discussion paper points out that some Member States already collect PNR data from other travelling forms than those used for air traffic.

The discussion paper is the outcome of a questionnaire on progress made in implementing Directive 2016/681, the results of which were presented during the Romanian Council Presidency in the first half of 2019. Accordingly, the majority of Member States favoured broadening the scope of data collection to other types of transportation (87% to maritime, 76% to railway, 67% to road traffic) but also stressed that the EU Directive on air traffic must be implemented first. Furthermore, any extension must ensure that the Passenger Information Units responsible for the PNR data base and data exchange can manage the additional data volume. (TW)

Council: The Way Forward in Data Retention

The Council remains committed to establishing a European regime on the retention of electronic communication data for the purpose of fighting crime. Following the conclusions on data retention drawn under the Austrian Council Presidency in December 2018 (see eucrim 4/2018, p. 201), the JHA Council again adopted conclusions in the matter at the end of the Romanian Council Presidency at its meeting on 6 June 2019.

The ministers restressed that "data retention constitutes an essential tool for law enforcement, judicial and other competent authorities to effectively investigate serious crime, […] including terrorism or cyber crime."

The ministers also acknowledged, however, that it is difficult to cut the Gordion knot, i.e. to bring up legislation that is in line with the EU's Charter on Fundamental Rights as interpreted by the European Court of Justice in the cases *Digital Rights Ireland* and *Tele 2 Sverige*. Despite further pending references for preliminary rulings against data retention rules (see eucrim 1/2019, p. 26), the Council feels that the legal possibility for data retention schemes at the EU and national levels should be maintained.

The Commission is invited to support the DAPIX-Friends of Presidency Working Party by gathering relevant information in the Member States and by means of targeted consultations of stakeholders. In particular, the Commission has been requested to get a comprehensive study off the ground to explore possible solutions for retaining data. The study may also serve as a basis for a future new legislative initiative on an EU data retention scheme. The conclusions stressed that the study must take into account the following issues:

- The evolving case-law of the Court of Justice and of national courts relevant for data retention;
- The outcomes of the common reflection process in the Council;
- Concepts of general, targeted and restricted data retention (first level of interference) and the concept of targeted access to retained data (second level of interference);
- Exploration of the extent to which the cumulative effect of strong safeguards and possible limitations at both interference levels could assist in mitigating the overall impact of retaining those data to protect the fundamental rights of the Charter, while ensuring the effectiveness of the investigations.

The Commission is further invited to report on the state of play of its work by the end of 2019. (TW)

Ne bis in idem

Art. 54 CISA and Red Notices: German Administrative Court Casts Doubt on Reliability of Interpol

Whether the maintenance of Red Notices by Interpol is in line with a person's right to free movement within the European Union is the subject of a reference for preliminary ruling by the Administrative Court of Wiesbaden, Germany, launched on 27 June 2019.

In the case at issue, a former manager of a large German company had been prosecuted for bribery acts allegedly committed between 2002 and 2007 in Argentina. While, in 2009, the public prosecutor in Munich discontinued proceedings once the defendant paid a certain sum of money determined by the prosecutor, parallel prosecutions were upheld in the USA. In particular, the U.S. prosecutor issued a Red Notice via Interpol seeking the arrest of the defendant and his surrender to the USA. In line with the CJEU's judgment in *Gözütok/Brügge* (Joined Cases C-187/01 and C-385/01), the German Federal Police Office (*Bundeskriminalamt*) informed Interpol that the defendant can no longer be prosecuted twice within the Schengen area pursuant to Art. 54 CISA, Art. 50 CFR. Interpol denied erasure of the Red Notice, however, because this can only

be carried out by the USA, which is not bound by Art. 54 CISA.

The defendant sued the Federal Police Office before the administrative court of Wiesbaden, seeking erasure of the Red Notice against him in the Interpol system. He argued that the decision of the public prosecutor in Munich unequivocally triggers application of the *ne bis in idem* rule pursuant to Art. 54 CISA/Art. 50 CFR, which is why he enjoys the right to free movement within the European Union and the Schengen area. However, he cannot exercise this right as long as the Red Notice is upheld in the Interpol system, because he must fear arrest and extradition to the USA by any other EU Member State if he leaves Germany. According to the defendant, compliance with the Red Notice by other EU Member States is illegal and unduly restricts his right to free movement.

Against this background, the administrative court of Wiesbaden referred several questions to the CJEU about the lawfulness of national law enforcement authorities processing Interpol Red Notices. The CJEU should, *inter alia*, clarify whether the right to free movement prohibits the person's provisional arrest in any other EU Member State if the country of origin (here: Germany) informed the states about the application of the Union-wide ban not to be prosecuted twice.

The court also casts doubt on whether Interpol has an adequate level of data protection or, at least, provides appropriate safeguards, so that the data transfer between Interpol and the EU Member States is legally possible in accordance with Arts. 36 and 37 of the EU's data protection Directive 2016/680. In general, the court questioned whether searches for arrest via Interpol can be processed by the EU Member States if they violate fundamental principles of Union law (here: free movement of person and *ne bis in idem* rule).

Put in focus: The reference is very interesting, since it tackles the more fundamental problem of the extent to which mutual recognition of Member States' judicial decisions are applied in favour of citizens ("reverse mutual recognition"). The CJEU must, however, also take into account international obligations of the EU Member States in this particular case. In addition, it must assess which legal consequences can be drawn from the fact that the US as a third state is not bound by the European *ne bis in idem* rule in Art. 54 CISA and Art. 50 CFR. (TW)

Victim Protection

Victims' Rights Directive: Commission Initiates Infringement Proceedings Against Nine Member States

On 25 July 2019, the Commission decided to open infringement proceedings against nine EU Member States for not having completely transposed Directive 2012/29/EU on the rights, support and protection of victims of crime. The so-called Victims' Rights Directive establishes EU-wide minimum standards for victims of crime as regards access to information, participation in criminal proceedings, and support and protection adapted to their needs. The Commission blames the Member States for not having implemented several provisions of this Directive, such as the right to be informed about both the victims' rights and the case, or the right to support and protection.

The Commission launched the first phase of the infringement procedure by sending a letter of formal notice to the Czech Republic, Estonia, Germany, Hungary, Italy, Malta, Poland, Portugal, and Sweden. The Member States must now answer the request within two months. If the Commission is not satisfied with the information and concludes that the Member States in question are failing to fulfil their obligations under EU law, the Commission may then send a formal request to comply with EU law (a "reasoned opinion"). (TW)

Cooperation

Police Cooperation

Prüm Cooperation: Agreements with Switzerland and Liechtenstein

On 27 June 2019, the EU signed agreements with Switzerland and Liechtenstein allowing the two countries to participate in the police cooperation scheme established by the so-called Prüm decisions. The agreement with Switzerland was published in the Official Journal L 187 of 12 July 2019, p. 3; the agreement with Liechtenstein was published in the Official Journal L 184 of 10 July 2019, p. 3.

The core of the Prüm legal framework is the speedy and efficient exchange of police information, especially as regards DNA profiles, dactyloscopic data (fingerprints), and data on vehicles and their owners. Police authorities from the participating countries are able to swiftly check whether data on any person or item is already stored in the database of another Prüm state. The Prüm legal framework consists of the following:

- Council Decision 2008/615/JHA ("the Prüm Decision"), which was adopted in order to incorporate into the EU legal framework the substance of the provisions of the previous Prüm Treaty on the stepping up of cross-border cooperation, particularly on combating terrorism, cross-border crime and illegal migration (the Treaty had been agreed upon by seven European countries in 2005);
- Council Decision 2008/616/JHA ("the Prüm Implementing Decision") laying down the necessary technical provisions for the implementation of Decision 2008/615/JHA;
- Council Framework Decision 2009/905/JHA laying down requirements for the exchange of DNA and fingerprint data in order to ensure that the results of laboratory activities carried out by accredited forensic service providers in one Member State are recog-

Report

Europäisches Strafrecht nach der österreichischen Ratspräsidentschaft

Konferenz der Österreichischen Vereinigung für Europäisches Strafrecht

On 7 March 2019, the Austrian Association of European Criminal Law together with the Vienna University of Economics and Business and the Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice organized a one-day conference on "European Criminal law after the 2018 Austrian Presidency of the Council of the European Union". The event raised great interest by many scholars and practitioners and covered three main topics:

- **The exchange of electronic evidence with regard to the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters;**
- **Mutual trust or mistrust among the EU Member States under consideration of the protection of fundamental rights;**
- **Current developments in substantive European criminal law.**

Am 7. März 2019 veranstaltete die Österreichische Vereinigung für Europäisches Strafrecht gemeinsam mit dem Institut für Österreichisches und Europäisches Wirtschaftsstrafrecht der Wirtschaftsuniversität Wien und dem Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz (BMVRDJ) eine Konferenz zum Thema „Europäisches Strafrecht nach der österreichischen Ratspräsidentschaft". Die Veranstaltung wurde von zahlreichen nationalen und internationalen Strafrechtsexperten aus Wissenschaft und Praxis besucht.

Die Moderatoren Univ.-Prof. Dr. *Robert Kert*, Univ.-Ass. Dr. *Andrea Lehner* sowie Staatsanwältin Dr. *Madalena Pampalk-Lorbeer* führten durch einen Tag voller spannender Vorträge, angefangen mit dem Themenblock „E-Evidence: Grenzüberschreitende Ermittlungen von elektronischen Beweismitteln: Gegenseitige Anerkennung auf neuen Wegen oder Abwegen?". Eingeleitet wurde dieses Themengebiet mit einer lebhaften Eröffnungsrede des Generalsekretärs im BMVRDJ Sektionschef Mag. *Christian Pilnacek*, der insbesondere auf die Erfolge verwies, die während der österreichischen Ratspräsidentschaft auf dem Feld der E-Evidence erzielt werden konnten. Die besonders große praktische Bedeutung von elektronischen Beweismitteln in der Zukunft sowie das Bedürfnis der Strafverfolgungsbehörden auf solche Beweismittel, die etwa in Clouds gespeichert sind, zugreifen zu können, wurden von Staatsanwältin Dr. *Judith Herrnfeld* (BMVRDJ) und Professor Dr. *Martin Böse* (Universität Bonn) analysiert. Dr. *Herrnfeld* stellte den Vorschlag für eine Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und die während der österreichischen Präsidentschaft erzielten Verhandlungsergebnisse vor. Prof. Böse nahm den Entwurf aus kompetenz- und grundrechtlicher Sicht kritisch unter die Lupe. Dr. *Christof Tschohl* setzte sich in seinem Vortrag vor allem mit möglichen Grundrechtseingriffen durch die Erlangung von E-Evidence auseinander. Abgerundet wurde der erste Themenblock durch die Darstellung der Sicht der Dienstanbieter von Dr. *Maximilian Schubert* (Internet Service Providers Austria).

Im zweiten Themenblock ging es um das gegenseitige Vertrauen oder Misstrauen zwischen den Mitgliedsstaaten im Rahmen der justiziellen Zusammenarbeit und die Wahrung der Grundrechte durch die Mitgliedsstaaten der Europäischen Union. Dr. *Albin Dearing* (Europäische Agentur für Grundrechte) erläuterte das Spannungsverhältnis zwischen wechselseitigem Vertrauen und nationaler Souveränität in der grenzüberschreitenden Zusammenarbeit von Justizbehörden, während Oberstaatsanwalt Mag. *Wolfgang Pekel* (BMVRDJ) über die Förderung der gegenseitigen Anerkennung durch die Stärkung des gegenseitigen Vertrauens im Rahmen der justiziellen Zusammenarbeit sprach. Schließlich präsentierte Dr. *Roland Kier*, Strafverteidiger und Vorstandsmitglied der European Criminal Bar Association, die Vorstellungen von Grundrechtsschutz aus Sicht der Verteidigung.

Im dritten Themenblock zu aktuellen europäischen Entwicklungen im materiellen Strafrecht gab zunächst der leitende Staatsanwalt Dr. *Christian Manquet* (BMVRDJ) ein Update zur Bekämpfung des Missbrauchs unbarer Zahlungsmittel. Schließlich präsentierten er und Mag. *Stefanie Judmaier* (BMF) die im österreichischen Recht geplanten Änderungen aufgrund der Richtlinie über die strafrechtliche Bekämpfung von EU-Betrug.

Intensive und auch emotionale Diskussionen zeigten, dass europäische Einflüsse auf das Strafrecht nicht nur für den Gesetzgeber, sondern auch für die Praxis große Herausforderungen und vielfältige Problemstellungen mit sich bringen. Die Tagung bot ein Podium, um gemeinsam Lösungen zu überlegen und zu diskutieren.

Carmen Kaudela & Lena Radl, Wirtschaftsuniversität Wien

nised by the relevant authorities as being equally reliable as the results of laboratory activities carried out by forensic service providers accredited in any other Member State.

The agreements with Switzerland and Liechtenstein specifically regulate which provisions of the above-mentioned decisions are applicable in bilateral relations between the Swiss Confederation/the Principality of Liechtenstein and each of the EU Member States. The agreements also provide for rules on the uniform application and interpretation of the referred provisions, dispute settlement, consequences of amendments to the Prüm legal framework, and the relationship with other cross-border cooperation agreements. Before the agreements enter into force, the EU, on the one hand, and Switzerland and Liechtenstein respectively, on the other, must notify each other of completion of the procedures required to express their consent to be bound by the agreements.

Although often called "Schengen III," the "Prüm cooperation" is not part of the

Schengen Acquis, which is why Schengen-associated countries can only join on the basis of separate agreements with the EU. The Schengen states Norway and Iceland already concluded similar agreements in 2009 (not ratified yet) that would allow them to participate in data exchange under Prüm. (TW)

Judicial Cooperation

Finnish Council Presidency: Alternatives to Detention as Partial Solution for More Effective Mutual Recognition

The Finnish Council Presidency, which began on 1 July 2019, continued discussions initiated by previous presidencies on how more effective judicial cooperation in criminal matters can be ensured and how current obstacles to the implementation of the principle of mutual recognition can be overcome. One particular focus is on alternatives to detention, which could solve the problem of poor prison conditions and prison overcrowding – a persisting problem that undermines mutual trust and hampers mutual recognition.

The Finnish Council Presidency tabled the discussion paper "Future of Justice. Detention and its Alternatives", which aims at launching a debate on how decisive steps can be taken at the EU level in order to eliminate the problem of prison conditions. The paper emphasises that detention should be used as a last resort and that criminal sanctions must be both effective and proportionate. Legal acts, e.g., Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgements and probation decisions with a view to the supervision of probation measures and alternative sanctions, EU policy programmes, resolutions by the European Parliament, and Council conclusions acknowledge the importance of alternatives to detention, but shortcomings still exist. The paper further stresses that a sustainable solution must be found, and synergies should be strived for with the Council of Europe and other organisations.

The Justice Ministers of the EU Member States held a first policy debate on the issues mentioned in the paper of the Finnish Presidency at their informal meeting in Helsinki on 19 July 2019. Points of discussion were as follows:

- Role of alternative sanctions in the countries' criminal policy;
- Best practices worth being shared among the EU Member States;
- Potential policy agreement on a long-term commitment by the EU Member States, the Commission, and the Council of Europe to tackle all obstacles to judicial cooperation in criminal matters;
- Potential policy agreement on the use of alternative sanctions as a partial solution to the problems of mutual recognition and prison overcrowding;
- Role of the EU in supporting efforts by the Member States to reduce prison overcrowding.

The discussions will continue at subsequent JHA Council meetings. (TW)

Council: The Way Forward in the Field of Mutual Recognition in Criminal Matters

The Austrian Council Presidency triggered a debate in 2018 on how mutual trust – as underlying element of mutual recognition – can be put back on a solid basis. The Romanian Council Presidency continued the debate on the future of mutual recognition in criminal matters. Following the Council conclusions on mutual recognition in December 2018 (see eucrim 4/2018, pp. 202–203), it compiled a report giving an overview of the current challenges in EU judicial cooperation in criminal matters. In the light of this report, a policy debate was held at the JHA Council meeting on 6 June 2019.

The report summarises the answers provided by the EU Member States in response to the discussion paper "the way forward in the field of mutual recognition of judicial decisions in criminal matters, responding to the necessity of avoiding impunity and observing procedural safeguards," which was launched in February 2019. The discussion paper and report deal with the following four points of discussion:

- Challenges encountered in application of the criteria set out in the Aranyosi judgment or when applying grounds for non-recognition in mutual recognition instruments;
- Training and guidance on mutual recognition instruments;
- Identification of gaps in the application of mutual recognition instruments and possible ways to fill these gaps;
- Enhancing the institutional framework, allowing for proper functioning of judicial cooperation in criminal matters at the EU level and making comprehensive use of this institutional framework.

The Romanian Presidency included several recommendations on each discussion issue. Regarding challenges, for instance, the creation of a common working methodology/common guidelines is suggested that looks at the application of the two-step approach established by the *Aranyosi* judgment in practice, and, in particular, the request for information about prison conditions.

As regards the identification of gaps in the application of mutual recognition instruments, the report concludes that most practitioners are of the view that the EU's judicial cooperation instruments are comprehensive enough, but it is necessary to enhance the application of existing instruments and to improve practitioners' knowledge through continuous training and awareness raising. (TW)

Infringement Proceedings Against Ireland for Failure to Transpose Several Mutual Recognition Instruments

On 25 July 2019, the Commission sent reasoned opinions to Ireland for having failed to transpose a number of framework decisions strengthening judicial cooperation in criminal matters and implementing the principle of mutual recognition. The instruments concerned are:

- Recognition of judgments imposing custodial sentences (Framework Decision 2008/909/JHA);
- Probation measures and alternative sanctions (Framework Decision 2008/947/JHA);
- Supervision measures (Framework Decision 2009/829/JHA);
- Financial penalties (Framework Decision 2005/214/JHA);
- The exchange of criminal records information (Framework Decision 2009/315/JHA);

The Commission noted that Irish authorities have not provided satisfactory answers on completion of the ongoing legislative implementation procedures. Ireland now has two months to comply with the concerns raised by the Commission. Otherwise, the Commission may refer the case to the European Court of Justice.

As regards the Framework Decision 2008/909 on the recognition of judgments imposing custodial sentences, the Commission also sent a reasoned opinion to Bulgaria for not having adopted the necessary legislation transposing the FD. (TW)

European Arrest Warrant

Clarifying the Concept of 'Issuing Judicial Authority' under the EAW

In reaction to the judgments of the CJEU in joined cases C-508/18 (OG) and C-82/19 PPU (PI) and case C-509/18 (PF) on the interpretation of the concept of „an issuing judicial authority" within the meaning of Art. 6(1) Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between the Member States (FD EAW), Eurojust has set-up a questionnaire to assess the situation in the Member States. The compilation of replies with a country-by-country overview was now published in order to support national authorities in the Member States with the execution of EAWs.

Member States give further information with regard to five questions, namely:
- Whether public prosecutors can issue an EAW in their countries?
- Which entity ultimately takes the decision to issue an EAW?
- Whether public prosecutors under their national law afford a guarantee of independence from the executive so that they are not exposed to the risk of being subject, directly or indirectly, to directions or instructions in a specific case from the executive, e.g. a Minister for Justice, in connection with the adoption of a decision to issue an EAW?
- Is the Member State affected by the CJEU's judgments and which legal and/or practical measures has been taken or will be taken in order to prevent and address this issue?
- Are there any other additional comments to be shared with the other Member States in view of the judgment?

All EU Member States provided replies to the questionnaire that may further be updated in the future. (CR)

Follow-up to the CJEU's Judgments on the Concept of "Issuing Judicial Authority"

On 27 May 2019, the CJEU delivered its landmark judgments in the case C-509/18 (PF) and Joined Cases C-508/18 (O.G.) & C-82/19 PPU (P.I.), clarifying the criteria as to when public prosecution offices can be regarded as judicial authority within the meaning of Art. 6(1) FD EAW, meaning that they are entitled to issue EAWs (see eucrim 1/2019, pp. 31–34). In the Joined Cases C-508/18 & C-82/19 PPU, the CJEU denied the necessary independence of German public prosecution offices and cancelled their judicial authority status in the sense of the FD. As for the "Lithuanian case" (C-508/18), the CJEU left the final assessment to the referring Irish court.

Following the judgments, Austria, Denmark, Italy, and Sweden issued notes clarifying the status of their public prosecution offices, which are to be regarded as judicial authorities in the opinion of these Member States. The notes are available on the EJN website.

Germany, which is directly and most greatly affected by the judgments, also issued a note It, *inter alia*, states: "[…] Germany will adjust the proceedings to issue a European Arrest Warrant. From now on, European Arrest Warrants will only be issued by the courts. This can be achieved without changing the existing laws. We have already informed the courts and public prosecutors about the ECJ judgement." Germany will also review its notification on Art. 6(1) FD EAW.

Nonetheless, practice in Germany remains confused at the moment. Some local and regional courts have rejected public prosecutors' applications to issue EAWs for lack of a legal basis. Other courts broadly interpret the provisions on arrest notices in the German Code of Criminal Procedure and affirm the court's competence to issue EAWs.

For the possible impact of the CJEU's judgments on the hotly debated e-evidence proposals, see the CCBE statement of 29 May 2019 under "Law Enforcement Cooperation". (TW)

CJEU: Executing MS Must Ensure Enforcement of Foreign Custodial Sentences Against Residents – *Poplawski II*

In a judgement delivered on 24 June 2019 in case C-573/19, the CJEU made fundamental statements on consequences of the primacy of Union law, the importance of interpretation in conformity with Union law, and the extent of limits to these principles. The legal background was shaped by Framework Decision 2002/584 on the European Arrest Warrant (FD EAW). The case concerned the enforcement of a custodial sentence imposed by a Polish court in the Netherlands that denied the surrender of Polish citizen *Daniel Adam Poplawski* to Poland, because he is considered a resident in the Netherlands (refusal ground of Art. 4 No. 6 of the FD EAW)

The case at issue follows a first judgment of the CJEU in the same case (judgment of 29 June 2017, C-579/15 – *Poplawski I*), in which the Court held that Dutch legislation establishing only a "willingness" to take over the sentence, if the optional refusal ground of Art. 4 No. 6 FD EAW is applied, is contrary to EU law. Furthermore, the 2017 judgment called to mind the obligation of national courts to interpret domestic law, so far as possible, in accordance with that framework decision (for details, see eucrim 2/2017, pp. 74–75).

By its second reference for a preliminary ruling, the *Rechtbank Amsterdam* essentially enquired whether it must disapply the national provisions in conflict with the FD EAW if it is unable to fulfil the obligation to interpret its domestic law in compliance with EU law.

In its answer of 24 June 2019, the CJEU first reestablishes the fundamental principle of the primacy of Union law over national law. It also reiterates the duties of national courts to give full effect to the provisions of EU law. However, a provision of EU law that has no direct effect cannot be the basis for disapplying a national law that conflicts with it. This is the case for framework decisions adopted on the basis of the former third pillar (Art. 34(2)(b) EU). Therefore, the referring court "is not required, solely on the basis of EU law, to disapply a provision of its national law which is contrary to those framework decisions."

The CJEU stresses, however, that the binding character of framework decisions places on national authorities/courts an obligation to interpret national law in conformity with EU law "to the greatest extent possible." Such interpretation in conformity with EU law has (only) two limits:

- The principles of legal certainty and non-retroactivity preclude the establishment of criminal liability of individuals being determined or aggravated, on the basis of a framework decision alone;
- Conforming interpretation would lead to an interpretation of national law contra legem, i.e., the obligation to interpret national law in conformity with EU law ceases when the former cannot be applied in a way that leads to a result compatible with that envisaged by the framework decision concerned.

In the present case, the CJEU believes that both limits do not apply. In particular, the Dutch court would be able to treat the FD EAW as a formal basis for applying the Dutch law allowing the execution of a foreign sentence to be taken over.

Furthermore, the FD EAW stipulates that the executing authority may only refuse surrender on the basis of Art. 4 No. 6 FD EAW if assurance is given that the custodial sentence passed in the issuing State against the person concerned can actually be enforced in the executing Member State. In this context, the CJEU emphasizes the paramount importance of avoiding all risk of impunity for the requested person.

As a result, the referring court is required to interpret its national law to the greatest extent possible, in conformity with EU law, which enables it to ensure an outcome that is compatible with the objective pursued by the FD EAW. (TW)

European Investigation Order

Guidance on Application of the EIO

The EJN and Eurojust published a joint note on the practical application of the EIO. The document aims at providing guidance to practitioners on the practical application of the EIO by looking at the issuing phase, the transmission phase, the recognition phase, and the execution phase. The note provides additional information on the scope of the Directive, its use in comparison to other co-existing legal instruments, on competent authorities, the use of a number of specific investigative measures. It also addresses the content, form, and language of the EIO. The note is based on information gathered by Eurojust and the EJN from meetings, documents, and casework. For a recent meeting report on the EIO by Eurojust, see eucrim 1/2019, p. 37 and the article by *Guerra/Janssens* in the same issue at pp. 46–53. (CR)

Criminal Records

EU Creates New Central Database for Convicted Third Country Nationals

spot light

The European Parliament and the Council have established the legal framework that will facilitate the exchange of information on past convictions of third-country nationals (TCNs). The framework consists of the following legal acts:

- Regulation (EU) 2019/816 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, published in the Official Journal L 135, 22.5.2019, p. 1;
- Directive (EU) 2019/884 amending Council Framework Decision 2009/315/JHA as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, published in the Official Journal L 157, 7.6.2019, p. 143.

The new legislation responds to the problem that the current legal framework on the European Criminal Records Information Exchange System (ECRIS), which was put in place in 2012, does not sufficiently address the particularities of requests concerning third-country nationals. Since conviction information on TCNs are currently not stored in the single repository of ECRIS, Member States are obliged to send "blanket requests" to all other Member States in order to determine whether and in which Member State a particular TCN was convicted. According to the Commission, this administrative burden deters Member

States from requesting information on non-EU citizens via the network. For background information on the legislative proposal launched by the Commission in 2017, see eucrim 3/2017, p. 120.

Regulation 2019/816 now establishes a centralised system at the Union level containing the personal data of convicted third-country nationals ("ECRIS-TCN"). ECRIS-TCN will allow the central authority of a Member State to promptly and efficiently find out in which other Member States criminal records information on a third-country national is stored so that the existing ECRIS framework can be used to request the criminal records information from those Member States in accordance with Framework Decision 2009/315/JHA.

ECRIS-TCN works on a "hit/no hit" basis, i.e., the system consists of the identity data (alphanumeric and biometric data) of all TCNs convicted in the Member States. A search mechanism allows Member States to search the index online. A "hit" identifies the Member State(s) that have convicted a particular TCN. The identified Member State(s) can then be requested to provide full criminal records information through the established ECRIS.

The main features of the ECRIS-TCN Regulation are:

- Personal data related to citizens of the Union who also hold the nationality of a third country and who were subject to a conviction will be included into ECRIS-TCN. The conditions for the inclusion of fingerprint data of Union citizens is different than those for persons who have only the nationality of a non-EU country;
- ECRIS-TCN allows for the processing of fingerprint data and facial images for the purpose of identification;
- The Regulation provides for minimum rules according to which fingerprint data must be collected and entered into the system;
- In a first phase, facial images may be used only to confirm the identity of a third-country national who has been identified as a result of an alphanumeric search or a search using fingerprint data. After technical readiness, facial images can also be used for automated biometric matching.
- The use of ECRIS-TCN is not only limited to getting criminal record information for the purpose of criminal proceedings against the person concerned, but also the following purposes (if provided for under and in accordance with national law) are covered by the Regulation:
  - Checking a person's own criminal record on his/her request;
  - Security clearance;
  - Obtaining a licence or permit;
  - Employment vetting;
  - Vetting for voluntary activities involving direct and regular contacts with children or vulnerable persons;
  - Visa, acquisition of citizenship and migration procedures, including asylum procedures;
  - Checks related to public contracts and public examinations;
  - Other purposes decided by the Member States (which must be notified to the Commission and published in the Official Journal).
- Eurojust, Europol, and the EPPO are allowed direct access to ECRIS-TCN in order to fulfill their tasks and to identify those Member States holding information on previous convictions of third-country nationals. If there is a "hit" indicating the Member States holding criminal records information on a third-country national, Eurojust, Europol, and the EPPO may use their respective contacts to the national authorities of those Member States to request the criminal records information (in the manner provided for in their respective founding legislative acts).
- Eurojust will additionally function as a central hub for information requests, addressed by third countries and international organisations, as to which Member States, if any, hold criminal records information on a third-country national.
- Retention period: Each data record will be stored in the central system for as long as the data related to the convictions of the person concerned are stored in the criminal records.
- ECRIS-TCN records can be made for convictions both after and prior to the start date for data entry;
- The Regulation establishes strict rules on access to ECRIS-TCN and the necessary safeguards, including the responsibility of Member States when collecting and using the data. It also specifies how individuals may exercise their rights to compensation, access, rectification, erasure, and redress, in particular the right to an effective remedy and the supervision of processing operations by independent public authorities.

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) has been mandated with the development and operation of ECRIS-TCN. After the technical and legal arrangements have been made, the Commission will set the date for the operational start of the system.

Directive 2019/884 effects the Regulation and introduces necessary modifications to the basic ECRIS act, i.e., Framework Decision 2009/315/JHA. The Directive obliges Member States to take necessary measures to ensure that convictions are accompanied by information on the nationality/nationalities of the convicted person if they have such information at their disposal. It also introduces procedures for replying to requests for information, ensures that a criminal records extract requested by a third-country national is supplemented by information from other Member States, and provides for the technical changes that are necessary to make the information exchange system work.

The Directive also incorporates into said Framework Decision the principles of Decision 2009/316/JHA which, to date, contains the regulatory framework for building and developing the computerised system for the exchange of infor-

mation on convictions between Member States.

The establishment of the new, central EU database ECRIS-TCN also raised criticism. Some stakeholders, such as the Meijers Committee and Statewatch, voiced concern as to whether the inclusion of persons holding both EU and non-EU citizenship (dual nationals) is in line with the principle of non-discrimination. Another question was whether the inclusion is proportional, because a factual basis is lacking that Member State authorities really become aware of the person's dual citizenship. The possibility to enter facial image data was also seen critically, since the actual ECRIS framework does not provide for this. Initially, MEPs took a critical stance on these issues but later gave up their opposition. (TW)

Law Enforcement Cooperation

E-Evidence: Commission Obtains Mandates for EU-US Agreement and Negotiations in Council of Europe

After the respective recommendations put forward by the Commission (see eucrim 1/2019, p. 41), the Council gave two mandates to the Commission to negotiate on behalf of the EU agreements on access to e-evidence. The mandates endorsed on 6 June 2019 refer to:

- Conclusion of an agreement between the Union and the United States of America on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider;
- Participation in the negotiations in the Council of Europe on a second additional protocol to the Cybercrime Convention.

The Council also set up negotiation directives to guide the Commission when conducting the negotiations. These directives are set out in addenda documents to the Council decision on the mandate and, *inter alia*, include the safeguards that the Council wishes to be included in the international rules on e-evidence. The Council particularly emphasised that the agreements must be compatible with the envisaged EU legal framework on e-evidence, which is currently being fiercely discussed in the Council and European Parliament (see eucrim 1/2019, pp. 38 ff.; eucrim 4/2018, pp. 206 f.).

The future EU-US agreement aims above all at setting common rules guaranteeing speedy access to content and non-content data, particularly those data stored in clouds on the servers of telecommunication service providers. It also aims at avoiding conflicts of law. To date, US-based service providers, who are the main addressee of the new regulations, only cooperate with EU law enforcement authorities on a voluntary basis and regularly limit access to non-content data. The new mandate will include rules that allow law enforcement orders to be sent directly to the service providers and short deadlines within which the requested data must be supplied. Realtime telecommunications data are not mentioned in the Council negotiating directives.

Likewise, the second additional protocol to the Budapest Convention on Cybercrime (CETS 185) aims at laying down provisions for a more effective and simplified mutual legal assistance (MLA) regime in cybercrime and e-evidence matters. The additional protocol is currently under discussion in the Council of Europe working parties. It will also include direct cooperation with service providers in other state parties to the Convention, and searches are to be extended across borders.

Both mandates underline that the Council must be closely involved in the preparation and conduct of negotiations by the Commission. To this end, it will be especially for the Finnish Council Presidency to fulfil these monitoring tasks in the second half of 2019.

Before an agreement can be signed and concluded, the Commission will have to obtain separate authorisation from Member States. The European Parliament must also be informed and will have to consent before an agreement can be signed and concluded. (TW)

Data Protection Authorities and EDPS Assess Impact of US CLOUD Act

Following a request to the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Data Protection Board (EDPB), and the European Data Protection Supervisor (EDPS) adopted a joint initial legal assessment of the impact of the US CLOUD Act on the EU legal data protection framework and the mandate for negotiating an EU-US agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters. The legal assessment focuses on compliance of the US CLOUD Act with the requirements of Arts. 6, 48, and 49 of the GDPR.

The CLOUD Act allows US law enforcement authorities to request the disclosure of data by service providers in the USA, regardless of where the data is stored (for details, see eucrim 1/2018, p. 36; eucrim 4/18 p. 207 and the article by *J. Daskal*, eucrim 4/2018, pp. 220–225).

In their reply to the LIBE Committee, the EDPB/EDPS stress that a future international agreement between the EU and the USA, for which the Commission recently obtained a negotiation mandate, must contain the following guarantees:

- Strong procedural and substantive fundamental rights safeguards;
- The necessary level of protection for EU data subjects;
- Legal certainty for businesses operating in both jurisdictions.

Furthermore, an "EU-level approach" is needed, which, *inter alia*, requires that U.S. law enforcement authorities be put on an equal footing with EU law enforcement authorities to obtain e-evidence.

Ultimately, the EDPB/EDPS also emphasise that there is an urgent need for a new generation of mutual legal assistance treaties that contain strong data

protection provisions, such as guarantees based on the principles of proportionality and data minimisation or the "criminality principle."

The legal assessment also summarises the replies of the EDPS of 2 April 2019 to the Commission regarding the planned EU-US e-evidence agreement (see eucrim 1/2019, p. 41). (TW)

CCBE: Legality of E-Evidence Proposal Even More Questionable After CJEU's Judgements on "Judicial Authorities"

In a statement of 29 May 2019, the Council of Bars and Law Societies of Europe (CCBE) looks into the impact of the CJEU's judgements of 27 May 2019 on the concept of judicial authority (case C-509/18 (PF) and Joined Cases C-508/18 (O.G.) & C-82/19 PPU (P.I.); see eucrim 1/2019, pp. 31–34) on the debated proposal for a Regulation on European Production and Preservation Orders for e-evidence in criminal matters. The CCBE argues that the exclusion of public prosecution offices not possessing the necessary independence (such as the German prosecution services) to be a judicial authority in the sense of the Framework Decision on the European Arrest Warrant underpins the arguments against the legality of the e-evidence proposal.

As outlined in the CCBE position paper of October 2018, it is highly questionable whether the proposed e-evidence Regulation can be based on Art. 82(1) TFEU. Art. 82 TFEU applies to cooperation between judicial authorities only. Now, however, nobody can be sure that a prosecutor who issues e-evidence production orders is considered a "judicial authority." For the ongoing debate on the e-evidence proposal, see the previous eucrim issues 1/2019 and 4/2018. (TW)

EU CTC: Influence of 5G Technology on Law Enforcement

At the JHA Council meeting of 7 June 2019, the EU Counter Terrorism Coordinator (EU CTC) updated ministers on the implications of the new generation of wireless technology 5G on law enforcement and judicial operations. In a paper drafted on 6 May 2019, the EU CTC highlighted that 5G is not a simple evolution of the previous 4G standard but it will change the telecommunications landscape and the life of citizens considerably (e.g., in view of interconnected or autonomous driving, telemedicine, smart cities, etc.). In addition to competitiveness, cybersecurity, technology, economic and geo-political issues, law enforcement, and judicial concerns must also be brought into the debate.

The EU CTC lists a number of challenges in connection with the 5G standard for law enforcement and judicial authorities, e.g.:

- Lawful interceptions of telecommunications will become more difficult, due to 5G's high security standards and a fragmented and virtualised architecture;
- Difficulties for the judiciary in establishing the authenticity of the evidence and distinguishing fake from real evidence, because multiple actors are involved in providing the 5G networks;
- Availability of the 5G-based networks in crisis situations.

The EU CTC also stressed that lawful interception in a 5G environment must be maintained, which necessitates urgent action, *inter alia*:

- Taking law enforcement concerns seriously, so that standardisation processes must be influenced by this perspective;
- Entering into dialogue with operators, so that configurations of the network can be designed specifically for law enforcement purposes;
- Member States and potentially the EU must reflect on appropriate legislation addressing the above-mentioned concerns.

Regarding the latter point, the EU CTC recommends, in particular, thinking of EU legislation to deal with cross-border aspects of lawful/real-time interception within the EU, because the new technology will increase the cross-border dimension of interception.

Ultimately, the EU CTC reflects on steps to be taken by the EU institutions, agencies, and bodies. He considers it important that heads of telecommunications interception units continue to meet regularly at Europol to exchange views on the law enforcement challenges related to 5G and to develop suggestions for solutions. National operators may be associated with this working group. In addition, law enforcement and judicial authorities must communicate with authorities responsible for cybersecurity, because their respective interests may be in conflict with each other. This could be accomplished within the framework of the meetings of the Heads of the Cyber Security Authorities of the Member States. The Commission could be invited to develop guidelines and explore legislative measures in order to avoid fragmentation. (TW)