News

Actualités / Kurzmeldungen

European Union*

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

Foundations

Fundamental Rights

FRA Looks into Facial Recognition Technology

At the end of November 2019, FRA published a paper looking into the fundamental rights challenges involved when public authorities deploy live facial recognition technology for law enforcement purposes.

According to the paper, the following key aspects should be considered before deploying facial recognition technology in real life:

- A clear and detailed legal framework should regulate the use of facial recognition technology and determine when the processing of facial images is necessary and proportionate;
- The processing of facial images for verification purposes should be clearly distinguished from the processing of facial images for identification purposes, as the risk of interference with fundamental rights is higher in cases of identification, which therefore requires stricter necessity and proportionality testing;
- Facial recognition technology is likely to raise fears of a strong power imbalance between the state and the individual and should therefore only be used in exceptional cases, i.e., to combat terrorism or to detect missing persons and victims of crime;
- The use of facial recognition technology during demonstrations may prevent people from exercising their freedom of assembly or association and should therefore be considered disproportionate or unnecessary;
- The risk of incorrectly flagging people must be kept to a minimum, and anyone who is stopped as a result of facial recognition technology must be treated in a dignified manner;
- Fundamental rights considerations, such as data protection or non-discrimination requirements, should be necessary requirements in the procurement of facial recognition technology;
- Public authorities should obtain all necessary information from the industry to carry out a fundamental rights impact assessment of the application of facial recognition technology they aim to procure and use;
- Close monitoring by independent supervisory bodies with sufficient powers, resources, and expertise should be guaranteed.

The FRA paper is a valuable tool for public authorities when considering fundamental rights implications in their plans to use the new technology in real life. (CR)

Area of Freedom, Security and Justice

Lisbon Treaty: 10 Years Area of Freedom, Security and Justice

On 1 December 2019, the new European Commission under the lead of its new President, Ms *Ursula von der Leyen*, marked the tenth anniversary of the entry into force of the Treaty of Lisbon. The 1st of December 2019 also marked ten years of the integration of the former intergovernmental cooperation scheme in justice and home affairs (the so-called third pillar of the Maastricht Treaty) into a full-fledged EU policy with the aim of establishing an area of freedom, security and justice. With the entry into force of the Lisbon Treaty, the EU Charter of Fundamental Rights also became legally binding.

The last ten years brought about a number of achievements in justice and home affairs, e.g.:

- Better connectivity of law enforcement authorities by means of the next generation of the Schengen Information System;
- Increased efforts in the fight against crime, including sexual abuse and ex-

* If not stated otherwise, the news reported in the following sections cover the period 16 November – 31 December 2019.

ploitation of children, trafficking in human beings, terrorism, and cybercrime;
- Completion of the instruments on judicial cooperation in criminal matters, e.g., the European Investigation Order, the European Protection Order, and the Regulation on Freezing and Confiscation;
- Improved data protection by means of the data protection law enforcement Directive (2016/680).

On the occasion of the ceremony, *Ursula von der Leyen* stated:

"There could be no better day for the new College of Commissioners to begin our work than this anniversary. Starting today, we are the guardians of the Treaties, the custodians of the Lisbon spirit. I feel this responsibility. It is a responsibility towards our predecessors, our founding fathers and mothers, and all that they have achieved. But it is also a responsibility towards our children. The responsibility to leave them a Union that is stronger than the one we have inherited." (TW)

Updates on Legislative JHA Items

The Finnish Council Presidency updated the JHA Ministers about the progress achieved on current legislative proposals in the area of freedom, security and justice during its presidency at the Council meeting on 2–3 December 2019. In the area of home affairs, the proposals include:
- Regulation on preventing the dissemination of terrorist content online;
- Home affairs funds (Asylum and Migration Fund, Internal Security Fund, Border Management and Visa Instrument Fund);
- ETIAS consequential amendments;
- Regulation on the False and Authentic Documents Online (FADO) system;
- Visa Information System (VIS) Regulation;
- Schengen Borders Code.

In the area of justice, progress on following files is reported (among others):
- Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-Evidence Regulation) and Directive on legal representatives for gathering e-evidence in criminal proceedings;
- Relevant funds (Justice Programme and the Rights and Values Programme);
- Directive on the Protection of persons reporting on breaches of Union law (Whistleblowing Directive). (TW)

Security Union

JHA Ministers Conclude Debate on Future of EU Internal Security

The Finnish Council Presidency summed up the outcome of discussions on the EU's way forward regarding internal security issues. The discussion was launched at the beginning of the Finnish Presidency in July 2019 (see eucrim 2/2019, p. 84). The final Presidency report was discussed at the meeting of the Justice and Home Affairs Ministers on 3 December 2019. The reflections detailed in the report contribute to the implementation of the strategic agenda 2019–2024 in the area of justice and home affairs. Future EU policy will concentrate on the following four issues:
- Proactive approach to new technologies: The EU needs an integrated and comprehensive approach in this field. An innovation lab is to be established within Europol in order to assess the needs for new technologies and their risks to law enforcement and to promote communication with the industry and academia. Law enforcement authorities should be involved at an earlier stage in the technological processes, which mainly take place in universities and the private sector. Moreover, the EU should take into account internal security and law enforcement interests in new legislation relating to new technologies.
- Effective information management: Future law enforcement cooperation will increasingly be based on information systems and their interoperability. Law enforcement authorities will have access to a much larger volume of data and information than ever before. Therefore, the EU must ensure that information systems are supplied with high-quality, timely, and complete data and are used effectively. The EU must also develop a clear vision on crime analysis; this includes the provision of sufficient human and financial resources to process and analyse information. In addition, the new EU interoperability framework must be used effectively, which necessitates appropriate and continuous training for the end-users.
- Multidisciplinary cross-border cooperation: The EU needs a horizontal, integrated, and coherent approach towards tackling the evolving, cross-cutting nature of security threats, such as CBRN weapons and hybrid activities. Therefore, the EU must ensure multidisciplinary, operational cooperation that goes beyond cross-border law enforcement cooperation, thus also involving other

Publication "European Union Instruments in the Field of Criminal Law and Related Texts"

In December 2019, the Council General Secretariat's Criminal Law Team published a compendium of selected texts on legal instruments (106 texts) relevant for EU criminal law. It includes instruments adopted by the EU Institutions on the following:
- Cooperation in criminal matters (including mutual recognition of judicial decisions);
- Instruments concerning substantive criminal law;
- Extracts from the Treaties;
- Agreements between the EU and third countries, such as those relating to mutual legal assistance.

In addition to an index, the publication also contains electronic bookmarks. By clicking on the links in the content section, the reader quickly arrives at the text he/she is looking for. The electronic version of the book (PDF) is available free of charge via the Council website > Documents & Publications. Hard copies are also available. (TW)

authorities, such as civil protection actors. It must also remove obstacles to operational cross-border cooperation, e.g., differences in national decision-making processes, legislation, and operating models; differences in national data collection and data processing practices; etc. Reflections on better methods of working together and the exchange of information involving new technologies should be intensified. This could, for instance, include unmanned autonomous systems, automatic number plate recognition technologies, and single-search interfaces for available databases. The EU should also aim towards a common law enforcement culture, which involves improving language skills, learning about each other's cultures, and exchanging best practices. Another field of action is the constant monitoring of the EU JHA agencies' tasks and responsibilities. Cooperation among them must be increased, as they will continue to play a significant role in the future. Adaptations to their legal framework must be assessed; in particular, Europol's legal base may be further adapted in view of the request and reception of personal data directly from private parties.

- Comprehensive approach to security: The security threat landscape is sure to change in the future. This requires better coordination, resources and technological capacities as well as a better situational awareness and preparedness. Hybrid threats, disinformation, use of new technology and the internet for criminal activities, violent radicalisation and right-wing extremism are the major challenging areas, which EU action should be focused on. (TW)

Salzburg Forum Declaration

On 6–7 November 2019, the Salzburg Forum met in Vienna/Austria. Austria briefed the home affairs ministers of the EU Member States at the JHA Council meeting on 2–3 December 2019 about the outcome of the meeting. The ministers for the interior at the Salzburg Forum launched a declaration that discusses the main challenges in home affairs policy at the regional level. In substance, the declaration deals with two issues: 1) human smuggling, borders, and security; 2) the functioning of the Dublin and Schengen systems.

As regards human smuggling, borders and security, the declaration calls on the European Union to focus more strongly on the fight against human smuggling along the Eastern/Central Mediterranean routes. The declaration points to bi-/multilateral cooperation in Central/Southeast Europe and to various agreements at the European and regional levels, which led to good progress in the fight against human smuggling and the enhancement of border protection. The Salzburg Forum also stressed that it is now time to take concrete operational measures, however, and made several proposals in this regard. Ultimately, cooperation along the Eastern Mediterranean route should become a best practice model for joint efforts in the fight against human smuggling. This would be a good contribution to the "Whole-of-Route" approach proposed by the Finnish EU Council Presidency.

As regards the Dublin/Schengen system, the declaration stresses that the EU's asylum system (based on the Dublin legal framework) is not working properly and that the Schengen system must be reinforced. The Salzburg Forum calls for a new approach to migration, which must include "rules on asylum and migration in the EU that are accepted, consistently implemented and enforced by all EU Member States." Moreover, the declaration sets out the goals and parameters by means of which the Forum will contribute to the new pact on asylum and migration, which will be drawn up by the new European Commission.

The Salzburg Forum is a Central European security partnership that was initiated by Austria in 2000. The main goal is to strengthen regional cooperation in the field of internal security. Fields of cooperation include:

- Illegal migration and asylum;
- Police cooperation;
- Information exchange;
- Cooperation in case of major events;
- Witness protection;
- The fight against drugs;
- Police training, etc.

The Member States of the Salzburg Forum are: Austria, Bulgaria, Croatia, the Czech Republic, Hungary, Poland, Romania, Slovakia, and Slovenia. Close dialogue is held with Western Balkan countries and Moldova. There are at least two Salzburg Forum Ministerial Conferences per year. (TW)

CJEU Rules on Public Security Measure within EU Competence on Approximation of Laws

On 3 December 2019, the CJEU dismissed an action of the Czech Republic that sought the annulment of Directive 2017/853 of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons. The case reference is C-482/17.

In view of the abolishment of the internal borders within the Schengen area, the 1991 Directive lays down the conditions under which various categories of firearms can be acquired and held for civil purposes as well as the requirements for the prohibition to acquire firearms for reasons of public safety. With the revision of 2017, the European Parliament and the Council introduced stricter rules for the most dangerous, deactivated, and semi-automatic firearms in response to terrorist acts and in order to prevent the misuse of firearms for criminal purposes.

The Court held that the measures taken by the European Parliament and the Council in the contested directive (Directive 2017/853) do not entail breaches of the principles of conferral of powers, proportionality, legal certainty, protection of legitimate expectations, and non-discrimination as alleged by the Czech Republic in support of its action.

First, the Czech Republic argued that the 2017 Directive could not be based

on Art. 114 TFEU (approximation of laws of the Member States in relation to the functioning of the internal market) because the main objective exclusively pursues a higher level of public security. Moreover, there is currently no legal basis in the Treaties for the adoption of the established prohibitions. Art. 84 TFEU specifically excludes harmonisation in the fields of prevention of crime and terrorism.

The CJEU held, however, that, where an act based on Art. 114 TFEU has already removed any obstacles to trade in the area that it harmonises, the EU legislator is not prevented from adapting that act to any change in circumstances or any development of knowledge with regard to its task of safeguarding the general interests recognised by the Treaty, e.g., the fight against international terrorism and serious crime in order to pursue public security. Moreover, the CJEU pointed out that the contested Directive cannot be regarded in isolation, but should include a look at the existing rules that it amends, which are important in order to identify the legal basis. Otherwise the paradoxical result would occur that the amendments could not be based on Art. 114 TFEU, whereas it would have been possible to achieve the same normative result by a full recast of the initial Directive. Ultimately, the CJEU cannot see that the contents of the contested Directive have nothing to do with the internal market. On the contrary, the 2017 Directive adjusts the balance between the free movement of goods and the security of EU citizens. In sum, there is no violation of the principle of conferral of powers.

Second, the Czech Republic argued that a breach of the principle of proportionality exists. In this context, the Czech Republic particularly blamed the EU institutions for not having carried out an impact assessment. In addition, it raised doubts as to whether the measures adopted are appropriate to achieve the objective of combating the misuse of firearms.

The CJEU, by contrast, found that the EU legislator has broad discretion when it makes political, economic, and social choices. This discretion is subject to a limited judicial review. The CJEU examined the 2016 Interinstitutional Agreement on Better Law-Making. Indeed, the Commission should, as a rule, carry out an impact assessment if a legislative initiative has significant economic, environmental, or social implications. However, not carrying out an impact assessment cannot necessarily be regarded as a breach of the proportionality principle. The EU legislator is only required to have sufficient information enabling it to assess the proportionality of a planned measure. Therefore, during the legislative procedure, co-legislators must take into account the available scientific data and other findings that became available, including scientific documents used by the Member States during Council meetings. The CJEU observed that the EU legislature had at its disposal numerous analyses and recommendations covering all the issues raised in the Czech Republic's argument. These analyses and recommendations did not prove a manifest inappropriateness in relation to the objectives of ensuring public safety and security for EU citizens and the functioning of the internal market in firearms for civilian use. As a result, the CJEU did not see a violation of the EU institution's wide scope of discretion.

In addition, the CJEU rejected specific arguments of the Czech Republic against certain provisions and found no breach of the principles of proportionality, legal certainty, and the protection of legitimate expectations of categories of owners or holders of weapons (potentially subject to a stricter regime under the contested directive).

Ultimately, the CJEU rejected the argument of the Czech Republic that the 2017 Directive is discriminatory because it includes a specific provision that is only valid for Switzerland (to which the Directive also applies as a Schengen country). This provision is a derogation from the general prohibition on converting automatic firearms into semi-automatic firearms. It takes into account the specific Swiss military system based on general conscription and having had in place over the last 50 years a transfer of military firearms to persons leaving the army. The Czech Republic argued that such derogation introduces unequal treatment between Switzerland and the other EU/EFTA Member States.

The CJEU found, however, that the principle of equality first requires establishing that Switzerland and the EU/EFTA Member States are in a comparable situation as regards the subject matter of this derogation. This is not the case here because Switzerland is able to trace and monitor the persons and weapons concerned due to its long-standing culture and tradition. Hence, the country fulfils the public security and safety objectives pursued by the contested directive. This cannot be assumed for the other Member States. (TW)

Legislation

Legal Practitioner Training in 2018

After the European Commission announced in December 2018 that the EU achieved its goals of training legal practitioners on EU law in 2017 already – two years ahead of schedule (see eucrim 1/2019, p. 10) – the Commission confirmed that even more records were broken in 2018. In 2018, more than 190,000 legal practitioners (judges, prosecutors, court staff, bailiffs, lawyers, and notaries) took part in trainings on EU law or the law of another Member State. Altogether, there was a 148% increase in training between 2011 and 2018. In total, more than one million legal practitioners have attended trainings on EU law since 2011. As in previous years, an upward trend in the number of participants and training activities since 2011 is noticeable. This trend especially applies to judges, court staff, and bailiffs in 2018.

These are the main results of the eighth Commission report on European judicial training in 2018, which was published at the end of December 2019. For the first time, the report includes the progression of the number of participants for the professions monitored over the last eight years; this is based on the European Commission Staff Working Document on the evaluation of the 2011–2020 European judicial training strategy. Other conclusions of the report are as follows:

- Although the absolute number of participants increased, there is a considerable difference if the percentage of participants is interpreted in relation to the total number of their profession;
- While over 63% of judges of the responding Member States received continuous training on EU law, for example, only 4,83% of lawyers in private practice did;
- Again, judges, prosecutors, and notaries received far more training on EU law or on the law of another Member State than members of other legal professions did;
- In Germany, for instance, nearly 80% of prosecutors were trained on EU law, but less than 10% of lawyers.

The Commission concedes, however, that the picture of the real training situation is incomplete due to data gaps. There is, for instance, a lack of data from private training providers for lawyers, which means this only allows for a limited assessment. Also, date collection varies from Member State to Member State and some Member States do not even respond to the questionnaire. The Commission concludes that the results nonetheless indicate differences in trainings between professions and Member States. There are still challenges ahead, most notably for lawyers, court, and prosecution office's staff and bailiffs' training. The lessons from the report and the above-mentioned strategy evaluation will feed into the Commission's reflection on the post-2020 strategy for European judicial training, which is currently being elaborated. (TW)

Institutions

Council

Croatian Presidency Programme

On 1 January 2020, Croatia took over the Presidency of the Council of the European Union. Under the motto "A Strong Europe in a World of Challenges," the Croatian Presidency's programme is built around four pillars

- A Europe that develops;
- A Europe that connects;
- A Europe that protects;
- An influential Europe.

Regarding judicial cooperation in criminal matters, the Croatian Presidency's priorities are to finalise the trialogue negotiations on the e-evidence package and to lay the necessary groundwork for the work of the European Public Prosecutor's Office. Furthermore, the Presidency will focus on implementation of the EU's existing legal instruments for judicial cooperation in criminal matters.

Priorities in the area of home affairs include migration management, external border protection and Schengen, the interoperability between information systems, and a comprehensive approach towards internal security, focusing on resilience to cyber-attacks, hybrid threats, and the dissemination of fake news.

Another focal point is the external dimension of justice and home affairs. In this regard, the Croatian Presidency strives to reach an agreement with the USA on the exchange of e-evidence, on intensifying joint efforts in the fight against terrorism through the exchange of information from conflict-affected areas, and on fighting serious international organised crime.

Further priorities in the area of justice include the development and promotion of e-Justice, digital platforms, and modern technologies; the continuation of discussions on improving the educational system for judicial officials in the EU; and finalisation of the Regulation establishing the Justice programme and the Regulation establishing the Rights and Values programme.

The Croatian Presidency is the third in the current trio Presidency, following Romania (January–June 2019) and Finland (July–December 2019). (CR)

OLAF

High-Level Conference on Customs Fraud in Helsinki

On 14–15 November 2019, the Finnish Customs and OLAF organised a high-level conference in Helsinki at which participants discussed current trends and appropriate responses to customs fraud. The event (entitled "Strategies to fight customs fraud in a globalised trading landscape") brought together national customs officials and representatives from EU bodies, including OLAF, Europol, Frontex, and the EU Intellectual Property Office (EUIPO). Discussions centred around the challenges of customs fraud, e.g., underevaluation, misdeclaration, and smuggling. They also included best practices on how to prevent, investigate, and detect customs fraud in the face of a growing volume of consignments, particularly as a result of the boom in e-commerce. (TW)

European Public Prosecutor's Office

State of Play in Establishing the EPPO

The justice ministers of the Member States were informed about the state of play of the implementation of the EPPO Regulation at the JHA Council meeting on 2/3 December 2019. The Commission regularly briefs the Council on the setting up of the new EU body. The most recent progress was summarised in a non-paper of 22 November 2019.

The press release on the December JHA Council meeting also reported

that the newly appointed EPPO Chief Prosecutor, Ms *Laura Codruța Kövesi*, who took office on 1 November 2019 (see eucrim 3/2019, p. 164), presented her vision and plans for the office. She stressed that work on several areas is necessary to achieve the objective of making the EPPO operational by the envisaged date, i.e., by the end of 2020. These include the:

- Implementation of the PIF Directive;
- National adaptations to the EPPO Regulation;
- Appointment of the European prosecutors to complete the constitution of the college;
- Agreement on the number of delegated prosecutors;
- A functional case management system.

She also highlighted the importance of providing the EPPO with adequate human and financial resources, so that it can fulfil its task efficiently. (TW)

Europol

Data Requests from Private Parties

At its JHA meeting on 2/3 December 2019, the Council adopted Conclusions on Europol's cooperation with private parties. While respecting the supporting role of Europol with regard to actions carried out by the competent authorities of the Member States, the Council acknowledges in its Conclusions the urgent operational need for Europol to request and receive data directly from private parties. Hence, it has called on the European Commission to take this into account as part of its review of the implementation of the Europol Regulation (EU) 2016/794. (CR)

Compliance with Terrorist Finance Tracking Programme Agreement

On 14 November 2019, the European Data Protection Supervisor (EDPS) published his inspection report on Europol's compliance with Article 4 of the TFTP Agreement (Agreement between the EU and the USA on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (O.J. L 195, 27.7.2010)). Europol's role under the Agreement is to make sure that the data on financial transfers requested by the US and stored in EU territory is necessary for the fight against terrorism and the financing of terrorism and that each request is defined as narrowly as possible.

In general, the report concludes that Europol does a good job of verifying US requests. Nevertheless, the report outlines eight recommendations for Europol to consider when carrying out these activities. The most important recommendation set forth by the EDPS is for Europol to be able to ask US authorities for additional information when checking that their requests actually meet necessity requirements in terms of countries and message types. Other recommendations concern, for instance, the verification process and security measures. (CR)

Eurojust

First Day as an Agency

On 12 December 2019, Eurojust officially became the European Agency for Criminal Justice Cooperation, with its new Regulation taking effect the same day (see also eucrim news of 18 February 2019).

Novelties set into motion under the Regulation EU 2018/1727 include a new governance structure (with an Executive Board of six members), new powers for the national Members, new procedures for the work of the College, and stronger democratic oversight. Relations with other institutions and agencies such as the EJN, Europol, and the EPPO have been set out. The types of serious crime for which Eurojust is competent now include genocide and war crimes.

In addition, Eurojust is now run by a new data protection regime, adapting it to the revised EU legal framework on data protection. The European Data Protection Supervisor (EDPS) is responsible for the external supervision of Eurojust, replacing the Joint Supervisory Body (JSB). While the UK and Ireland decided to opt-in to the Eurojust Regulation, Denmark is not bound by it. Hence, on 11 December 2019, a cooperation agreement between Denmark and Eurojust took effect (see eucrim news of 20 December 2019). (CR)

New Rules of Procedure

Following the entry into force of its new Regulation, the College of Eurojust adopted new rules of procedure for Eurojust on 20 December 2019. The rules of procedure outline further functions as well as the election and dismissal procedures of the President and Vice-Presidents of Eurojust. Furthermore, they regulate the meetings of the College, its quorum, and its voting rules.

The composition and functioning of the Executive Board as well as the appointment of the administrative director form another integral part of these rules. The rules of procedure also set forth rules for written and preparatory consultation procedures, working groups, and on how to handle declarations of interest, conflicts of interest, information duties, and resolutions of disagreements. (CR)

100 Action Days Coordinated by Eurojust

At the end of November, Eurojust had coordinated its 100th action days since 2011. The 100 action days resulted in 3355 searches; the seizure of more than €210 million in cash, luxury cars and jewellery; and halted criminal activities worth nearly €2 billion.

During the action days, national authorities are able to use a purpose-built coordination centre at Eurojust. There they have access to dedicated and secure lines of communication enabling them to simultaneously conduct arrests, searches, interviews of suspects and witnesses, seizures of evidence, and the freezing of assets in real-time across several countries.

Since the first action days held upon the initiative of the French Desk at Eurojust in 2011 and concerning the smuggling of irregular migrants, action days have been held for all sorts of serious crime: cybercrime, terrorism, environmental crime, THB, financial fraud, weapons trafficking, drug trafficking, and financial crime. The latter was the subject of the 100th coordination centre, unravelling massive trans-European pay TV fraud. (CR)

European Judicial Network (EJN)

Allocation of Cases to Eurojust and to EJN

On 5 November 2019, Eurojust and the European Judicial Network (EJN) published a joint report with the aim of assisting practitioners in determining whether a case should be directed to Eurojust or to the EJN.

The report outlines the following items:

- Criteria for assessing which agency should deal with a request for assistance;
- Use of the updated 2018 Joint Paper on the EJN and Eurojust "What can we do for you?" for redirecting cases;
- Steps to be taken upon receipt of a request from national authorities when it appears to be better suited to the another's competence;
- Steps to be taken by a national desk at Eurojust upon receipt of a request from another national desk that appears to better fall under the EJN's competence;
- Existence of national rules preventing the national desks at Eurojust from redirecting a case to the EJN once the case has been opened at Eurojust;
- Steps to be taken when a request has been addressed to both a national desk at Eurojust and an EJN contact point;
- Use of the Eurojust National Coordination System for case-distribution purposes;
- Added value of the EJN-Eurojust double-hat function to the distribution of cases;
- Liaison between the national desks at Eurojust and EJN contact points, with a view to reaching a common approach on complementarity;
- Best practices.

The report highlights that the assessment of whether a request should be dealt with by Eurojust or the EJN should be made on a case-by-case basis, taking into account first the complexity of the case, followed by its urgency, as the main criteria. (CR)

Frontex

New Frontex Regulation in Force

On 4 December 2019, the new Frontex Regulation (EU) 2019/1896 entered into force. The main features are summarised in the press release of 4 December 2019.

The Regulation includes the following strengthening objectives for Frontex:

- Develop integrated planning such as capability development planning, contingency planning, and operational planning;
- Be capable to conduct operations in non-EU countries not neighbouring the EU;
- Upgrade its management system;
- Continue to provide national authorities with operational support on land, at sea, and in the air;
- Provide experts and training in order to further contribute to the fight against cross-border crime;
- Continue to assist national authorities in effective returns of those persons not eligible to remain in the EU;
- Focus on post-arrival/post-return assistance;
- Provide ongoing situation monitoring at external borders, risk analyses, and information exchange on what is happening at the EU's borders and beyond;
- Engage at least 40 fundamental rights monitoring specialists to be involved in its operations.

The new Regulation also means that Europe's first uniformed service is in place. Furthermore, Frontex will work more closely with national authorities in order to better plan the EU's responses to challenges – rather than merely reacting to crises. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

EP Supports Planned EU Legislation against VAT Fraud in E-Commerce

On 17 December 2019, MEPs backed new EU legislation that aims at curbing VAT evasion in e-commerce. The legislation (one Directive and one Regulation) will require payment service providers to keep records of cross-border payments related to e-commerce and to make these data available to anti-fraud authorities. Anti-fraud authorities will have access to a new, central electronic storage system, so that they can better process payment data. Administrative cooperation among the Member States' tax authorities and payment service providers will also be strengthened. The EP made several proposals on the text in order to make information sharing and prosecution more effective.

The EP has only a consultative function on the pieces of legislation. The exclusive competence to adopt the texts lies with the Council. The latter already reached political agreement in November 2019 (see eucrim 3/2019, p. 169). The Commission tabled the proposals in December 2018. It is estimated that the EU loses €137 billion every year due to e-commerce VAT evasion. (TW)

Corruption

Eurobarometer Survey on Business Attitudes to Corruption

spot light

The majority of companies (51%) is sceptical that corruption is being tackled efficiently by law enforcement. This is one of the

main results of the Eurobarometer survey on the businesses' attitude towards corruption in the EU. It was published on 9 December 2019 (International Anti-Corruption Day). The survey interviewed 7722 businesses in all 28 EU Member States between 30 September and 24 October 2019. It is the fourth survey of this kind (the first one was conducted in 2013, the others in 2015 and 2017). For the 2017 survey, see eucrim 1/2018, p. 13. The surveys include a wide range of topics, e.g.:

- Problems encountered when doing business;
- Business' perception of the level of corruption in their country;
- The prevalence of practices leading to corruption;
- Corrupt practices in public tender and public procurement procedures;
- Investigation, prosecution, and sanctioning of corruption.

Although corruption is not ranked among the top concerns, corruption is seen as a problem by five in ten European companies. The majority of companies think that tax rates, fast-changing legislation and policies (63%), and the complexity of administrative procedures (62%) are the main problems when doing business. Nevertheless, there is wide divergence among the EU Member States. Whereas 88% of companies in Romania see corruption as a problem when doing business in their country, only 5% of companies do in Denmark.

Furthermore, the general businesses' perception of corruption has decreased compared to 2013 (63%, down from 75%). However, the results also vary among the Member States on this point: in 17 Member States, the feeling that corruption is a widespread problem in their country has decreased since 2017 – most considerably in Germany (-25%) – but increased in 11 countries. Other results of the survey are as follows:

- Favouring friends or family members in business and public institutions is by far the most frequently mentioned corrupt practice;
- Over seven in ten companies agree that too close links between business and politics in their country lead to corruption and that favouritism and corruption hamper business competition;
- 30% of companies believe that corruption has prevented them from winning a public tender/procurement contract;
- More than 50% of companies think that corruption in public procurement managed by national and regional/local authorities is widespread;
- 51% of companies feel that anti-corruption measures are not applied impartially.

The survey also gives the reader a look behind the scenes of different business sectors. In this context, the survey reveals that sector analysis indicates significant differences between the sectors as regards corruption. 38% of companies in the healthcare and pharmaceutical sector, for instance, consider corruption to be a problem when doing business, but only 31% do so in the energy industry. The energy industry is also the business with the lowest proportion (19%) of companies that assume corruption has prevented them from winning a public tender/procurement contract; by contrast, around 30% are convinced of this in the construction and telecom/IT sectors. All in all, corruption remains an issue for both large and small companies. (TW)

Money Laundering

Council Frames Future EU AML/CFT Policy

The ECOFIN Council adopted conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism at its meeting on 5 December 2019 in Brussels. The conclusions are a direct response to the new – more general – strategic agenda for 2019–2024, in which the European Council stated: "We will build on and strengthen our fight against terrorism and cross-border crime, improving cooperation and information-sharing, and further developing our common instruments." For the new strategic agenda, see eucrim 2/2019, pp. 86–87. The conclusions also build on the Commission's AML/CFT Communication and the related assessment reports of July 2019 (see eucrim 2/2019, pp. 94 et seq.).

The conclusions underline that "the fight against money laundering and terrorist financing remains a high priority for the European Union." They not only urge Member States to complete implementation of all relevant Union legislation in the area, but also set clear political guidelines for the European Commission. Hence, the conclusions call for stepping up the Union's AML/CFT legal framework in accordance with international standards as set out by the FATF and MONEYVAL. These standards should be incorporated into EU law in a timely and comprehensive manner. The Commission is particularly invited to do the following:

- Thoroughly assess, as a matter of priority, any possible restrictions stemming from existing legislation (or lack thereof) with regard to efficient information exchange and cooperation among all relevant competent authorities involved in the implementation and supervision of the Union's AML/CFT framework;
- Consider the possibility of creating a coordination and support mechanism for Financial Intelligence Units (FIUs);
- Explore actions to enhance the EU's AML/CFT framework, e.g., by considering to address some aspects with a regulation;
- Explore the opportunities and challenges of using technological innovation to combat money laundering;
- Explore the possibilities, advantages, and disadvantages of conferring certain responsibilities and powers for anti-money laundering supervision to a Union body with an independent structure and direct powers vis-à-vis certain obliged entities.

The Commission is also called on to

report on the outlined actions every six months, starting in June 2020. (TW)

Organised Crime

2019 EU Drug Markets Report

On 26 November 2019, Europol and the EMCDDA published their joint EU Drug Markets Report for the year 2019, looking at impact and driving forces behind drug markets, the main drug markets in the EU, and how to respond to drug markets. The report finds that the drug market is a major source of income for organised criminal groups (OCGs) in the EU, at a minimum estimated retail value of €30 billion per year.

The report also identifies the following:

- Illicit drugs represent the most valuable market for criminal organisations operating in the EU;
- About two thirds of those engaged in the drug trade are also involved in other criminal activities;
- There are signs of increasing competition between groups, leading to escalating violence within the EU drug market;
- Overall, drug availability in Europe, for both natural and synthetic drugs, remains very high;
- The European drug market is increasingly characterised by consumers having access to a wide variety of high-purity and high-potency products that, in real terms, are usually equivalent in price or even cheaper than they have been over the past decade;
- Developments in the area of precursors have been an important driver in the expansion of drug production;
- The drug market is becoming more globally connected and technologically enabled;
- OCGs are becoming more internationally connected, and they exploit the gaps/differences that exist in regulatory and drug control environments;
- The main drivers of market changes and new threats stem from opportunities arising from the existence of global commercial markets and the associated logistical developments and digitalisation within these markets;
- The drug market has become increasingly digitally enabled. Both the surface web and darknet markets are used for online drug sales, as are social media and mobile communication apps. Encryption and anonymised services are also being increasingly used by OCGs for secure communication in the trafficking and sale of illicit drugs;
- Levels of production, globally and in the EU, are very high;
- Cocaine production in South America and heroin production in Afghanistan are estimated to be at historically high levels;
- China has gained in importance as a source country for drug precursors and new psychoactive substances;
- Africa has grown in importance due to its growing role as a trafficking and transit area;
- Europe is also a major producer of cannabis and synthetic drugs for the EU market and is, to some extent, a global supplier of MDMA (ecstasy) and amphetamines;
- In some neighbouring countries, OCGs are closely linked to ethnically-based groups residing in the EU, which is changing the dynamics of drug supply.

To tackle the identified problems, the report sets forth the following main targets for action:

- Strengthen efforts to target top-level OCGs active in the global drug market;
- Reduce vulnerabilities at external borders;
- Focus on key geographical locations for trafficking and production;
- Invest in forensic and toxicological capacities;
- Address links to other important security threats;
- Raise awareness about the cost of drug-related violence and corruption;
- Develop response to digitally enabled drug markets;
- Act at the global level. (CR)

Cybercrime

Council Conclusions on Significance and Security Risks of 5G Technology

5G networks will become part of the crucial infrastructure for the operation and maintenance of vital societal and economic functions and a wide range of services essential for functioning of the internal market. The EU must maintain technological sovereignty, however, and promote its approach to cyber security in conjunction with future electronic communication networks. This is stressed in the conclusions "The significance of 5G to the European Economy and the need to mitigate security risks linked to 5G," as adopted by the Transport, Telecommunications and Energy Council at its meeting on 3 December 2019. The conclusions set out political guidelines on how the EU should manage the future innovative 5G technology. The Council not only points out the assets of 5G (among others, the aim to make the EU the leading market for the deployment of 5G networks and the development of 5G-based solutions), but also outlines the challenges stemming from 5G technology. Hence, safeguarding the security and resilience of electronic communications networks and services (in particular as regards 5G), following a risk-based approach, is considered important. Against this background, the Council has established the following guidelines:

- Swift and secure roll-out of the 5G networks across the EU, which is key to enhancing the EU's competitiveness;
- Building trust in 5G technologies is firmly grounded in the core values of the EU (e.g., human rights and fundamental freedoms, rule of law, protection of privacy, personal data, and intellectual property); in the commitment to transparency, reliability, and inclusion of all stakeholders and citizens; and in enhanced international cooperation;
- A comprehensive approach and effective and proportionate security measures, with a focus on security and pri-

vacy by design as integral parts of 5G infrastructure and terminal equipment;
- Addressing and mitigating the challenges for law enforcement (e.g., lawful interceptions);
- Putting in place robust common security standards and measures that must be ensured by all businesses involved;
- Mitigating not only risks of 5G by means of standardization and certification, but also by means of additional measures;

Both the Member States and the Commission (with the support of ENISA) are encouraged to work together in order to ensure the security and integrity of 5G networks. (TW)

Environmental Crime

EU Framework on Environmental Crime under Scrutiny

Ten years after the criminal law directives on environmental crime and ship source pollution were agreed upon, the EU is now carrying out a thorough evaluation and assessment of the legal framework. On 15 November 2019, the Council tabled the draft final report on the eighth round of mutual evaluations, which was devoted to the practical implementation and operation of European policies on preventing and combating environmental crime. The report summarises the main findings and recommendations and draws up conclusions in view of strengthening the prevention of and fight against environmental crime across the EU and internationally.

Since the range of offences covered by environmental crime is broad, the eighth round of mutual evaluations focused on those offences which Member States felt warranted particular attention, i.e., illegal trafficking in waste and illegal production/handling of dangerous materials. The evaluation involves a comprehensive examination of the legal and operational aspects of tackling environmental crime, cross-border cooperation, and cooperation with relevant EU agencies. Evaluation missions to individual Member States started in September 2017 and ended in February 2019. The evaluation missions resulted in detailed reports on each of the 28 Member States.

The general report underlines, *inter alia*, that environmental criminal offences in the examined areas remain undetected, as this type of crime is often "invisible." It is therefore considered a "control crime," which, as such, has to be tackled proactively. The report also includes several recommendations aiming at improving the situation when fighting environmental crime. Member States should, for instance, adopt a comprehensive national strategy setting out priorities to fight these crimes. Another weak point identified was the lack of statistical data on the crimes and of information on the flow of cases from administrative and law enforcement authorities. Therefore, Member States are called on to work out a method by which to collect systematic, reliable, and updated statistics in order to enable a strategic evaluation of the national systems.

In addition to the eight rounds of mutual evaluations, the Finnish EU Council Presidency intensified discussions on the adequacy of the current EU criminal law framework on environmental crime, with the aim of identifying areas in which further approximation of the Member States' criminal laws may be advisable. To this end, the Finnish Presidency presented a report on the "state of environmental criminal law in the European Union" on 4 October 2019.

The report lists relevant developments in the EU's environmental policy since the 2008 Directive on the protection of the environment through criminal law and the 2005 Directive on ship source pollution (amended in 2009). The report also summarises the input given at various meetings regarding further development of the EU's regulatory framework in the field of environmental criminal law. Discussions focused on the following topics:
- Areas of environmental crime where criminal activity is considered to be more frequent or serious;
- Successes and challenges in countering environmental offences;
- Possible additional minimum rules on criminal sanctions in the area of environmental crime;
- The clarity of environmental criminal law.

The justice ministers of the Member States took note of the draft final report on the eighth round of mutual evaluations and the Finnish Presidency report at their JHA Council meeting on 3 December 2019.

The Commission is currently also carrying out a comprehensive evaluation of the 2008 Environmental Crime Directive (cf. the evaluation roadmap). This evaluation seeks to collect a comprehensive set of data on the scale of environmental crime. It will analyse the effectiveness of the Directive's current scope and its consistency with other, relevant EU level legislation. Among others, the evaluation is based on a wide public consultation and on targeted consultations with experts and practitioners dealing with combating environmental crime. The results of the evaluation are expected to be published in spring 2020. (TW)

Procedural Criminal Law

Data Protection

Council Conclusions on Widening Scope of PNR Collection

The justice and home affairs ministers of the Members States adopted conclusions on widening the scope of PNR data at the JHA Council meeting on 2 December 2019. As reported in eucrim 2/2019, p. 105, the Finnish Presidency took the initiative of launching the debate on extending the scope of the EU's current PNR scheme to forms of transport other than air traffic, such as maritime or railway traffic. The conclusions point out

that, even though some Member States welcomed the initiative, other delegations voiced concern about the timing and potential legal, technical, and financial challenges. Therefore, the ministers are asking the European Commission to carry out a thorough impact assessment on widening the scope of the PNR concept. The aim of the impact assessment is to explore the necessity and feasibility of the collection, storage, and processing of PNR data from other cross-border travelling forms. The conclusions list several aspects in relation to legal, operational, and technical issues that the study must include. (TW)

Council Push on Data Retention to Fight Crime

The Council closely monitors progress made by the Commission in the implementation of Council conclusions on the retention of data for the purpose of fighting crime, which were adopted in June 2019 (see eucrim 2/2019, p. 106). At the JHA Council meeting of 2–3 December 2019, the ministers took note of the progress made and reiterated that the Commission should "pursue all efforts needed to achieve a satisfactory balance between privacy and security concerns at EU level." The conclusions of June 2019 attempt to find a way out of the impasse that occurred after the CJEU found the 2006 data retention directive and the national data retention regimes of the UK and Sweden to be incompatible with the EU's Charter on Fundamental Rights. The CJEU did not completely rule out a data retention system, but it must set clear and precise conditions. The conclusions encouraged the Commission to prepare a new legislative initiative, in particular by conducting targeted consultations with stakeholders and supporting a comprehensive study that looks after possible solutions. (TW)

EU-US Privacy Shield – Third Annual Review

Despite efforts made by the United States authorities and the European Commission to implement the EU-US Privacy Shield, e.g., *ex officio* oversight and enforcement actions, the European Data Protection Board (EDPB) still voiced concerns over adequate data protection that must be addressed by both the Commission and the USA. The EDPB adopted its third annual review on 12 November 2019.

The EU-US Privacy Shield is a legal framework that protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. In operation since 1 August 2016, it allows the free transfer of data to companies that are certified in the USA under the Privacy Shield. By now, more than 5000 companies are already certified under the Privacy Shield, having committed to complying with EU data protection standards. The Shield is reviewed each year. The Privacy Shield must be distinguished from the EU-US Data Protection Umbrella Agreement, which contains a set of data protection rules that apply to all transatlantic exchanges between criminal law enforcement authorities.

According to the EDPB report, the lack of substantial checks remains a particular concern as far as commercial aspects of the Privacy Shield are concerned. Onward transfers, which lead to transfers of data outside the jurisdictions of the American and EU authorities, require more substantial oversight.

As regards access by public authorities to data transferred to the United States under the Privacy Shield, the EDPB regrets the insufficient information basis, which makes it difficult to assess to what extent data are collected for national security purposes. In particular, there have been no follow-up reports by the US Privacy and Civil Liberties Oversight Board (PCLOB). Such reports would be helpful, for instance, to evaluate whether the collection of data under Section 702 FISA is indiscriminate or not and whether or not access is conducted on a generalized basis under the UPSTREAM program. Furthermore, the EDPB has the impression that the Ombudsperson is not vested with sufficient power to access information and to remedy non-compliance. Thus, the EDPB still cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights.

The Commission already concluded its assessment report (third annual review of the functioning of the EU-US Privacy Shield, COM(2018) 495 final) in September 2019. After taking the opportunity to better examine daily experience and practical implementation of the framework, the Commission came to the conclusion that a number of concrete steps should be taken so that the Privacy Shield functions more effectively. Several recommendations have been addressed to the U.S. Department of Commerce and the Federal Trade Commission.

In a joint statement of 13 September 2019, U.S. Secretary of Commerce, *Wilbur Ross,* and *Věra Jourová,* at the time EU Commissioner for Justice, Consumers, and Gender Equality, defended the EU-US Privacy Shield. They underlined that the Privacy Shield plays a vital role in protecting personal data and contributing to the $7.1 trillion economic relationships between the United States and Europe.

The third annual review of the Privacy Shield was debated in the EP's LIBE Committee on 9 January 2020. MEPs voiced severe criticism and pointed to shortcomings in the data protection of EU citizens. (TW)

CJEU Rules on Lawfulness of Video Surveillance in Residential Buildings

On 11 December 2019, the CJEU ruled that national provisions which authorise the installation of a video surveillance system on buildings, for the purpose of pursuing the legitimate interest of ensuring the safety and protection of individuals and property, without the consent of the data subjects, are not contrary to EU

law if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Art. 7(f) of Directive 95/46/EC.

In the case at issue (Case C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*), the referring Romanian Court had to deal with an action brought by an owner of an apartment located in a residential building. The apartment owner applied for an order that the association of co-owners take out of operation the building's video surveillance system and remove the cameras installed in the common parts of the building because the instalment is contrary to EU's data protection law (Art. 6(1) lit. c) and Art. 7 lit. f) Directive 95/46, and Arts. 7, 8, 52 of the Charter).

The CJEU stressed that video surveillance systems processing personal data are lawful under the following three conditions:

First, the data controller or by the third party or parties to whom the data are disclosed must pursue a legitimate interest. In the case at issue, this condition is generally fulfilled if the controller seeks to protect the property, health, and life of the co-owners of a building. The extent to which the interest must be "present and effective" at the time of data processing did not need to be decided by the CJEU because the video surveillance system was installed after thefts, burglaries, and acts of vandalism had occurred.

Second, personal data must be processed for the purpose of the legitimate interests pursued; it is settled case law in this regard that derogations and limitations in relation to the protection of personal data must apply only insofar as is strictly necessary. In other words, it must be ascertained that the legitimate data processing interests pursued by video surveillance cannot reasonably be as effectively achieved by other means that are less restrictive of the fundamental rights and freedoms of data subjects. In addition, the processing must adhere to the "data minimisation principle" enshrined in Art. 6(1) lit. c) of Directive 95/46. The CJEU considered the requirements in relation to proportionality to have been met in the present case because the co-owners had installed an intercom/magnetic card system at the entrance of the building as an alternative measure, which proved to be insufficient. The CJEU points out, however, that the referring court must assess whether aspects of the data minimisation principle were upheld, e.g., determine whether it is sufficient if the video surveillance operates only at night or outside normal working hours, and whether it blocks or obscures images taken in areas where surveillance is unnecessary.

Third, the referring court must ensure that the fundamental rights and freedoms of the person affected by the data protection do not take precedence over the legitimate interest pursued. This necessitates a balancing of opposing rights and interests, which depends on the individual circumstances of each particular case in question. According to the CJEU, the following guidelines come to the fore here:

- Member States cannot exclude (categorically and in general) the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in any particular case;
- Such balancing must take into account the seriousness of the infringement of the data subject's rights and freedoms. It is important whether the data are accessed from public or non-public sources. Processing of data from non-public sources implies that the infringement is more serious because information relating to the data subject's private life will thereafter be known by the data controller and possibly to third parties;
- Account must be taken, *inter alia*, of the nature of the personal data at issue, in particular of the potentially sensitive nature of these data, and of the nature and specific methods of processing the data, in particular of the number of persons having access to these data and the methods of accessing them;
- For the purpose of the balancing exercise, the data subject's reasonable expectations are also relevant, namely that his/her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data;
- Lastly, all these factors must be balanced against the importance (for all the co-owners of the building concerned) of the legitimate interests pursued in the instant case by the video surveillance system at issue, inasmuch as it seeks essentially to ensure that the property, health, and life of those co-owners are protected.

The final assessment of this balancing has been left to the referring Romanian court. (TW)

EDPS: New Proportionality Guidelines

On 19 December 2019, the European Data Protection Supervisor issued guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. The guidelines aim at providing policymakers and legislators with practical tools to help assess the compliance of proposed EU measures impacting the fundamental rights to privacy and the protection of personal data with the Charter of Fundamental Rights. Ideally, conflicts between data protection and priorities/objectives of measures are to be minimised at an early stage.

The guidelines offer a practical, step-by-step method by which to assess the proportionality of new legislative measures, providing explanations and concrete examples. They respond to requests from EU institutions for guidance on the particular requirements stemming from Art. 52(1) of the Charter. The guidelines also complement the EDPS' 2017 "Necessity Toolkit," which guides policymakers in applying the necessity test to new EU measures that may limit the fundamental rights to

the protection of personal data (see eucrim 2/2017, p. 72). (TW)

Victim Protection

Whistleblowing Directive Published

spot light

On 26 November 2019, Directive 2019/1937 "on the protection of persons who report breaches of Union law" was published in the Official Journal (L 305, p. 17). The European Parliament and the Council already agreed on the content of the Directive in April 2019. For the compromise reached on this directive, nicknamed "Whistleblower Directive," see eucrim 1/2019, p. 27 (with further references on the legislative process, which was closely monitored in eucrim).

The *material scope* of the Directive is limited to specific areas of Union law, where the Union legislator believes in enhancing enforcement if breaches of law are reported. Still, the areas covered by the Directive are broad, including, e.g., public procurement, financial services, product and transport safety, protection of the environment, etc. Union acts that may be breached are set out in the annex to the Directive. The Directive expressly states that protection of the Union's financial interests is a core area of the Directive's scope, which is related to the fight against fraud, corruption, and any other illegal activity affecting Union expenditure, and the collection of Union revenues and funds or Union assets.

Legislation in the field of whistleblowing entails a number of legal problems regarding the *relationship with existing reporting mechanisms and conflicting areas*, e.g., the protection of classified information, the protection of legal/medical professional privilege, the secrecy of judicial deliberations, and rules of criminal procedure. The relationships in this regard are set out by the Directive. It also stresses that the Directive's provisions do not affect the Member State's responsibility to ensure *national security*. In particular, it shall not apply to reports of breaches of the procurement rules involving defence or security aspects unless they are covered by the relevant acts of the Union.

Regarding the Directive's *personal scope*, it broadly applies "to reporting persons working in the private or public sector who acquired information on breaches in a work-related context." The Directive lists a number of persons who must be included in the protection scheme at least, e.g.:

- Persons having the status of workers in the sense of Union law (including civil servants);
- Persons having self-employed status;
- Shareholders;
- Members of the administrative, management, or supervisory bodies of an undertaking, including non-executive members;
- Volunteers and trainees;
- Any persons working under the supervision and direction of contractors, subcontractors, or suppliers;
- Persons whose work-based relationship has since ended or is yet to begin (e.g., cases in which the information on breaches was obtained during the recruitment process or other pre-contractual negotiations);
- Facilitators and third persons who are connected with the reporting person (such as colleagues or relatives) and the legal entities owned by, or otherwise connected to, the reporting person in a work-related context.

However, persons may benefit from the protection under the Directive only if
(1) They had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this Directive; and
(2) They reported either internally in accordance with Article 7 or externally in accordance with Article 10, or made a public disclosure in accordance with Article 15.

The latter refers to the *reporting system* established by the Directive. The provisions mainly follow the flexible approach pushed through by the European Parliament. Accordingly, Member States shall "encourage" reporting through *internal* reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation. However, a whistleblower may also choose to *directly report* breaches to competent authorities. The Directive sets out the obligations, the necessary framework, the procedure, and the follow-up for both the internal and external reporting channels. This includes the obligation for companies with at least fifty workers to establish such channels and procedures for internal reporting and for follow-up.

Public disclosure (i.e., making information on breaches available in the public domain) – the third form of reporting – is protected by the Directive under the following conditions:
(1) The person first reported internally and externally, or directly externally, but no appropriate action was taken in response to the report within the timeframe referred to in the Directive; or (!)
(2) The person had reasonable grounds to believe that:
(i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or
(ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.
Member States have the duty to ensure that the *identity* of the reporting person is *not disclosed* to anyone beyond the authorised staff members competent to receive/follow up on reports, without the explicit consent of that person. By way of derogation, the identity of the report-

ing person may be disclosed if this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including those with a view to safeguarding the rights of defence of the person concerned. In these cases, safeguards also apply to the reporting persons, e.g., he/she must be informed before his/her identity is disclosed, and he/she must receive a written explanation of the reasons for the disclosure.

Another key element of the Directive involves *protection measures against retaliation*. This includes obligations for Member States to prohibit any form of retaliation against whistleblowers. In this context, the Directive provides a non-exhaustive list of prohibited retaliatory acts. It includes not only work-related measures, e.g., suspension/dismissal, demotion, or withholding of promotion, but also acts harming the whistleblower's reputation, blacklisting, and psychiatric or medical referrals.

Beyond the prohibitions, Member States are obliged to proactively take the necessary measures to ensure that the whistleblower is protected from retaliation. Such measures include the following:

- Persons who report breaches or publicly disclose them shall not be considered to have breached any restriction on disclosure of information and shall not incur liability of any kind in respect of such a report or public disclosure, provided that they had reasonable grounds to believe that the reporting or public disclosure of such information was necessary to reveal a breach pursuant to this Directive;
- Reporting persons shall not incur liability in respect of the acquisition of or access to the information reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence;
- If whistleblowers suffered a detriment, it shall be presumed that the detriment occurred in retaliation for the report or public disclosure (inversion of the onus of proof);
- Provided that they had reasonable grounds to believe that the reporting or public disclosure was necessary to reveal a breach, reporting persons can seek dismissal of legal proceedings, including those for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for compensation claims based on private, public, or on collective labour law;
- If information includes trade secrets, but the reporting person meets the conditions of the Directive, such reporting or public disclosure shall be considered lawful.

Furthermore, the Directive requires Member States to make available a number of support measures to whistleblowers, e.g.:

- Comprehensive and independent information and advice on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned;
- Effective assistance from competent authorities;
- Access to legal aid in accordance with EU law (i.e., Directive (EU) 2016/1919 and Directive 2008/52/EC applicable in criminal and in cross-border civil proceedings) and national law.

Ultimately, Directive 2019/1937 obliges Member States to provide for "effective, proportionate and dissuasive *penalties*" applicable to natural or legal persons who hinder or attempt to hinder reporting; retaliate or bring vexatious proceedings against whistleblowers; or breach the duty of maintaining the confidentiality of their identity. In addition to compensating damages, effective, proportionate, and dissuasive penalties must also be put in place against reporting persons who knowingly reported or publicly disclosed false information.

The Directive only establishes minimum rules, i.e., Member States can introduce or retain more favourable rules on whistleblowers' protection. They may also extend protection as regards areas or acts not covered by the Directive (see above for the material scope). Member States must implement the Directive by 17 December 2021. Regarding the obligation for legal entities in the private sector with 50 to 249 workers to establish internal reporting mechanisms, Member States have time until 17 December 2023. (TW).

Council Conclusions on Victims' Rights

The Finnish EU Council Presidency addressed the subject of victims' rights. During the Presidency, delegations of the EU Member States agreed on conclusions on victims' rights that were adopted at the JHA Council meeting on 2–3 December 2019. The conclusions first take stock of the comprehensive EU framework in this field, including legislative and non-legislative measures. Second, they outline how the existing EU framework can be strengthened, more efficient implementation can be improved/made, and the way forward be developed. The conclusions identify concrete actions and initiatives to be taken by the Commission and the Member States.

The European Commission is invited to draw up an EU strategy for 2020–2024 on victims' rights (for a corresponding demand by the Special Advisor, see eucrim 1/2019, p. 27). The strategy should be comprehensive and cover all victims of crime, with a special emphasis on victims of violent crimes. It should include a systematic approach to ensure victims' effective access to justice and compensation. The Commission should also evaluate the existing legislation. The evaluation should particularly focus on a review of the established compensation scheme, such as the 2004 Directive relating to compensation to crime victims.

EU agencies, such as Eurojust, FRA, the European Institute for Gender Equality and the European Network on Victims' Rights (ENVR) are invited to examine how to improve cooperation between competent authorities concern-

ing victims of violent crime in cross-border cases.

Member States are called on, *inter alia*, to ensure the complete and correct transposition and effective practical implementation of the existing EU legislation on victims' rights. Member States should also strive for involving all actors likely to come into contact with victims (comprehensive and holistic approach). The functioning of national compensation policies must be improved. (TW)

Cooperation

Police Cooperation

Council Gives Green Light for UK Exchange of Fingerprint Data via Prüm Network

On 2 December 2019, the JHA Council formally approved the United Kingdom's participation in the Prüm fingerprint exchange system. After having concluded that the UK has fully implemented the general provisions on data protection for the purpose of Prüm automated data exchange with regard to dactyloscopic data, the UK is, in principle, ready to exchange fingerprint data with the other EU Member States that are part of the Prüm network.

Council Decision 2008/615/JHA provides for the automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data (VRD) for the purpose of prevention and investigation of criminal offences and subject to certain conditions and procedures. The Council Decision transferred into EU law a former convention concluded outside the EU framework in Prüm, a German village. The convention strived for enhancing police cooperation between some EU Member States. After having opted-out from the Council Decision in 2014, but having rejoined it in 2016, the UK applied for being part of the data exchange system. According to said Council Decision, the supply of personal data for a specific Member State needs prior evaluation and is subject to a decision of the Council.

In its conclusions, the JHA Council stresses, however, that, "by 15 June 2020, the UK review its policy of excluding suspects' dactyloscopic files. If by then the UK has not notified the Council that it is making these data available, the Council will within three months review the situation with a view to the continuation or termination of Prüm automated dactyloscopic data exchange with the UK." Despite this warning, a real operational start is still dependent on an implementation decision, which the Council must take after consultation of the European Parliament.

How the EU and the UK will proceed if the UK leaves the EU is not mentioned in the Council conclusions and other EU documents.

In technical terms, both searches of the UK and searches by the UK will require the establishment of a technical interface with every other EU Member State – a process that can take years to complete, as Statewatch reported.

Statewatch also points to the fact that – if operable – the UK will provide fingerprints from nine million convicted individuals to the Prüm network, i.e. 98% of the total number of individuals whose fingerprints are stored in the UK Police National Computer. (TW)

Judicial Cooperation

Council Conclusions on Alternative Measures to Detention

One of the topics high on the agenda of the Finnish EU Council Presidency in the second half of 2019 was the debate on alternative measures to detention (see eucrim 2/2019, p. 109). The topic concerns EU policy debate since many years, but gained increased attention in the last years when prison overcrowding and bad prison conditions in some EU Member States have undermined mutual trust and thus have hampered judicial cooperation between the EU Member States (see also, for instance, eucrim 3/2019, pp. 177–178 [the *Dorobantu* case]). At its meeting on 2–3 December 2019, the ministers for justice of the Member States adopted conclusions on alternative measures to detention. The conclusions identify a number of concrete actions to be taken at the national level, the EU level and the international level. Member States are encouraged to do the following:

- Explore the opportunities to enhance, where appropriate, the use of non-custodial sanctions and measures, such as a suspended prison sentence, community service, financial penalties, and electronic monitoring (and similar measures based on emerging technologies);
- Consider enabling the use of different forms of early or conditional release;
- Consider the scope for and benefits of using restorative justice;
- Provide for the possibility to apply non-custodial measures also in the pre-trial stage of criminal proceedings;
- Ensure that information concerning the legislation on non-custodial sanctions and measures is easily available for practitioners throughout criminal proceedings;
- Provide adequate legal training to practitioners;
- Improve practical training notably as regards the use of EU instruments designed to prevent detention in cross-border situations, i.e. Framework Decision on probation and alternative sanctions (2008/947/JHA) and Framework Decision on European supervision order (2009/829/JHA);
- Pay particular attention to the needs of vulnerable persons, e.g. children, persons with disabilities and women during pregnancy and after giving birth;
- Improve capacity for probation services;
- Share best practices.

Regarding the EU level, particularly the Commission is invited to:

- Increase awareness of the benefits of non-custodial sanctions and measures

among policy-makers and practitioners;
- Carry out a comparative study to analyse the use of non-custodial sanctions and measures in all Member States so as to support the dissemination of national best practices;
- Enhance the implementation of the mentioned two Framework Decisions;
- Develop training for judges and prosecutors through the European Judicial Training Network (EJTN), as well as for prison and probation staff through the European Penitentiary Training Academies (EPTA);
- Launch regular experts' meetings on detention and non-custodial sanctions and measures.

Regarding the international level, the conclusions mainly emphasise the importance of close cooperation with the Council of Europe, so that synergies can be found. The Commission and the Member States should consider ways in which to promote the dissemination of the Council of Europe standard-setting texts, the relevant ECtHR case law and the CPT recommendations regarding detention and the use of non-custodial sanctions and measures. (TW)

FRA Report on Detention Conditions– New Tool for Legal Practitioners Dealing with EAWs

spot light

In December 2019, FRA published a report on criminal detention conditions in the EU. The report responds to the Commission's request to compile certain basic information on prison conditions and existing monitoring mechanisms in Member States. FRA stresses that the report does not intend to compare and rate EU Member States, but instead aims at assisting judges and legal practitioners in their assessment of mutual recognition instruments, in particular the European Arrest Warrant. The question of when the execution of an EAW can be denied because of bad prison conditions is a persistent problem (see, recently, the CJEU judgment in Case C-128/18, reported in eucrim 3/2019, pp. 177–178; see also the seminar report on the EAW AWARE project in this issue).

The report looks at five core aspects of detention conditions in EU Member States:
- Cell size;
- Amount of time detainees can spend outside of their cells, including outdoors;
- Sanitary conditions;
- Access to healthcare;
- Whether detainees are protected from violence.

For each of these aspects, the report gives an overview of the minimum standards at the international and European levels and explains how these standards are translated into national laws and other rules within the EU Member States.

Regarding cell space, the report concludes that the problem of overcrowding is a persistent issue in many EU Member States, despite the establishment of detailed minimum standards and guidelines on prison cell space at national, European, and international levels.

While serious issues can also be found in many Member States with regard to hygiene and sanitary conditions, the report notes a gradual improvement in the situation in prison facilities in the EU.

Regarding time spent outside cells and outdoors, the report finds that inmates benefit from only one hour a day outside their cells. Consequently, lock-up times last up to 23 hours per day, which is considered intolerable.

Looking at inmates' access to healthcare, the report states that all Member States provide medical services on the premises of detention facilities. However, the report also finds that a shortage of medical staff often leads to delays in medical examinations.

Lastly, the report finds inter-prison violence a cause for extreme concern – it is a critical issue in most Member States.

The report complements FRA's database on detention conditions. The database centralizes national standards, jurisprudence, and monitoring reports on detention conditions in all 28 EU Member States (see separate news item). (CR)

New Online Database on Conditions and Monitoring of Criminal Detention

FRA offers a new database on detention conditions in all 28 EU Member States on its website. This new Criminal Detention Database 2015–2019 offers information about selected core aspects of detention conditions such as cell space, sanitary conditions, access to healthcare, and protection against violence.

The database contains detailed information on the relevant case law of the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) as well as monitoring reports and statements of various national, European, and international bodies on detention conditions in the EU Member States. Furthermore, the database offers country-specific information, e.g., legal standards at the national level and who the responsible authorities for executing the EAW are.

The database is targeted at judges and legal practitioners involved in cross-border cases. It aims at serving as a "one-stop-shop" for practitioners seeking information about criminal detention conditions in any given EU Member State. The database is complemented by the FRA report on detention conditions in the EU, which was published in December 2019 (see separate news item). (CR)

EU-US Reaffirm Their Partnership to Tackle Security Threats

On 11 December 2019, representatives of the European Union – including new Commissioner for Justice, *Didier Reynders*, and the Finnish and Croatian ministers of justice and of the interior on behalf of the current and incoming Council Presidencies – met in Washington D.C. with U.S. Attorney General *William Barr* and Acting Secretary for Homeland Security *Chad Wolf* for the EU-U.S. Ministerial Meeting on Jus-

tice and Home Affairs. The Ministerial Meeting is held twice a year in order to oversee transatlantic cooperation in the area of Justice and Home affairs and address common security threats.

The December meeting was the first EU-U.S. Ministerial Meeting after the EU started its new political cycle. Both sides reaffirmed their strong commitment to foster the transatlantic partnership and pursue their dialogue on Justice and Home Affairs, building on the existing operational cooperation and best-practice exchanges on matters of common interest. The following issues were discussed and considered as priority areas for future cooperation:

- Regarding the fight against terrorism (which remains the top common priority), both sides consider important the sharing of information gathered in zones of combat for use in criminal proceedings as admissible evidence. In this context, continued operational cooperation between the relevant agencies, including Europol, was highlighted;
- By referring to the EU-U.S. PNR agreement, the use of Passenger Name Records (PNR) for the purpose of preventing, detecting and investigating terrorist offenses and related travel also remains important. The EU and the U.S. will work together in order to establish ICAO standards on PNR for law enforcement purposes implementing United Nations Security Council Resolution 2396;
- Hybrid threats and risks related to new emerging technologies, in particular 5G, are the main area in which cooperation will be fostered, so that the partners can react to the changing environment of security threats;
- The U.S. and the EU will join their efforts to establish rules on lawful access for law enforcement authorities to digital evidence, including when encrypted or hosted on servers located in another jurisdiction;
- Resilience to combat interferences into electoral processes will be strengthened;

The next EU-U.S. Ministerial Meeting will be held in the first half of 2020 in Croatia. (TW)

European Arrest Warrant

CJEU Clarifies Its Case Law on Concept of "Judicial Authority" Entitled to Issue EAWs

spot light

On 12 December 2019, the CJEU provided further guidance under which conditions public prosecutor's offices can be regarded as "issuing judicial authority" within the meaning of Art. 6(1) of the 2002 Framework Decision on the European Arrest Warrant (FD EAW). Uncertainties were triggered after the CJEU's judgments of May 2019, in which the Court found that the German public prosecutor's offices are exempt from the concept of "issuing judicial authority" because they may be subject to directions or instructions from the executive. The Court distinguished this case from the Prosecutor General of Lithuania who was considered a "judicial authority" that can issue EAWs, under the condition that his/her decisions are subject to court proceedings fully meeting the requirements inherent to effective judicial protection. For these landmark judgments, see eucrim 1/2019, pp. 31–34.

➤ *The Cases at Issue*

In the three cases decided on 12 December 2019, courts in Luxembourg and the Netherlands, which had to deal with the execution of EAWs, casted doubts whether the requirements set up in the decisions of May 2019 are met in view of the French, Swedish and Belgian public prosecutor's offices. The cases are referred to as follows:

- Joined Cases C-556/19 PPU and C-626/19 PPU (French Public Prosecutor's Office);
- Case C-625/19 PPU (Swedish Prosecution Authority);
- Case C-627/19 PPU (Belgian Public Prosecutor's Office).

While the cases on EAWs issued by the French and Swedish public prosecutor respectively concern EAWs for the purpose of conducting criminal prosecutions, the "Belgian" case concerned an EAW issued for the purpose of enforcing a criminal judgment.

➤ *Questions by the Referring Courts*

Regarding the French public prosecutor's office, the referring courts considered the following problems that may undermine the required independence in accordance with the CJEU's case law:

- Although the French Ministry of Justice cannot direct instructions in specific cases, it may issue general instructions on criminal justice policy;
- The issuing French public prosecutor is subordinate to his/her hierarchical superiors, and is therefore obliged to follow instructions/directions;
- He/she is, at the same time, the competent prosecuting body and the authority that controls the conditions for issuing EAWs and their proportionality, which raises doubts on impartiality.

In addition, the referring Dutch court observed that there is no separate legal remedy for the person concerned against the decision to issue an EAW and its proportionality. Instead, the public prosecutors rely on the decision of the (investigative) judge who examines the lawfulness of the issuance of the national arrest warrant. This argument was also put forward as regards the Swedish public prosecutor who issues EAWs after the criminal first instance court had ordered pre-trial detention against the suspect.

➤ *The CJEU's Arguments Regarding the French and Swedish Public Prosecutor's Offices*

Referring to its judgments of May 2019, the CJEU clarified that the examination of whether an authority participating in the administration of criminal justice – but which is not a judge or court – capable in an EU Member States to issue EAWs falls under the concept of "judicial authority" within the meaning of the FD EAW requires a two-step approach. First, it must be examined

Report

AWARE: Seminar on the European Arrest Warrant and Conditions of Detention

Bremen/Germany, 24–26 October 2019

On 24 to 26 October 2019, the Higher Regional Court of Appeal (*Oberlandesgericht*) in Bremen/Germany, together with the Bremen Ministry of Justice and Constitution, held a three-day seminar as part of an EU Justice Programme-funded series of three seminars looking at use of the European Arrest Warrant (EAW AWARE). The seminar in Bremen was attended by 38 European judicial and legal practitioners and academics from eight EU Member States.

The purpose of the seminar series is to incorporate different perspectives stemming from practitioner experience in order to address the challenges of EAW implementation and policy: decision-making information, use of existing provisions in national law, and informal judicial cooperation. A particular focus is on the obligations of the executing Member State courts to examine the detention conditions in the issuing Member States, alongside broader issues involving the protection of human rights of the requested person.

Following a welcome from Secretary of State for Justice for the Federal State of Bremen, *Björn Tschöpe*, practitioners heard from *Daniel Burdach* from the Registry of the European Court of Human Rights (ECtHR) regarding the ECtHR's rulings on the standards for prison detention conditions under the European Convention of Human Rights. Raising awareness among national executing judges for existing tools and the ECtHR's benchmark criteria are key goals of the EAW AWARE seminars. Mr. *Burdach* presented a detailed review of cases pertaining to the major problems of overcrowding and inappropriate detention facilities; he concluded by listing existing resources on the ECtHR factsheets and on the HUDOC database. In the afternoon session, Dr. *Klaus Schromek,* Presiding Judge at the Bremen Higher Regional Court of Appeal, provided European practitioners with broader context on criminal procedure in Germany. His colleague Dr. *Ole Böger* focused on the relevance of human rights protection in application of the EAW in the case law of European and domestic courts. He highlighted that both the European Court of Justice (ECJ) – especially in the *Aranyosi and Căldăraru* case (C-404/15), which had been initiated by a referral for a preliminary decision by the Bremen Higher Regional Court of Appeal – and the German Federal Constitutional Court require the courts of the executing Member States to ensure the human rights protection of the requested person in the issuing Member State. Dr. *Böger* also discussed remaining issues concerning the precise scope and content of these duties on the part of the executing Member States' courts, also referring to practical solutions for the future, e.g., enhanced databases and the facilitation of closer co-operation between judicial authorities of the issuing and executing Member States.

The first day of the seminar was concluded by Dr. *Ralf Riegel*, Head of the International Criminal Law Division at the German Federal Ministry of Justice and Consumer Protection, who led an engaging debate on the need for reform of the national and the international basis in EAW proceedings. Dr. *Riegel* tackled practical concerns of EAW proceedings both in the issuing state (such as use of a central EAW authority) and in the executing state (for instance, at which point and under what conditions representation by legal counsel should be organised).

Bearing in mind this focus on detention conditions, participants made onsite visits to both Bremen Correctional Facility and Bremen Secure Treatment Unit of the Psychiatric Treatment Centre. They heard first-hand accounts from staff, and the visits fueled the discussion that detention conditions are not to be understood as either an "east vs. west" issue or as the fault of unwilling regimes. Instead, improved conditions depend on investment and the capacity for renovation, and improvements must often accommodate changing factors such as new demographics. All this within the uniquely challenging requirements of a secure environment. The onsite visits ultimately led to a better understanding of the human rights relevance of detention conditions, with a particular emphasis on the need for open communication between the relevant authorities in the European spirit of mutual trust and cooperation.

Additional afternoon sessions were conducted, according to a prioritised agenda, including the following:

- Analysis of the German *Puigdemont* case and its reception in Spain (Mr. *Florentino Ruiz Yamuza*, Judge in Huelva/Spain);
- Rejection of surrender and problems/practice in relation to the enforcement of foreign sentences in Germany (Mr *Christian Schierholt*, Chief Senior Public Prosecutor, Celle/Germany);
- Extradition and Fair Trial, focusing on the ECJ's judgment in "LM" (C-216/18) and its reception in EU Member States from a comparative law perspective (Mr. *Thomas Wahl*, Senior Researcher at the Max Planck Institute for Foreign and International Criminal Law, Freiburg/Germany);
- The perspective of suspects and lawyers on extradition proceedings, with a focus on possibilities for avoiding detention (Dr. *Anna Oehmichen,* defence lawyer from Knierim & Kollegen, Mainz/Germany).

By bringing users of the EAW tool together with such a diverse, practical agenda, these seminars are designed to support, discuss, and build mutual trust and recognition of decisions between neighbouring European judiciaries and to promote consistent use of European bodies. The second seminar will take place in Bucharest/Romania from 23 to 27 March 2020 and the third in Lisbon/Portugal from 28 September to 2 October 2020. Persons and institutions interested in the material developed during EAW AWARE are warmly encouraged to get in touch with *Rhianon Williams* (rhianon.williams@justiz.bremen.de).

Rhianon Williams, EAW AWARE Project Coordinator within Bremen Ministry of Justice

Report

The 2019 Annual Conference on International Extradition and the European Arrest Warrant

Lake Iseo, Italy, 24–25 June 2019

25 law professors and practising lawyers from around the world gathered in Sarnico, Italy in the last week of June 2019 to brainstorm on current developments in extradition law and the practice of the European Arrest Warrant (EAW). The meanwhile fourth edition of the annual conference on International Extradition and the EAW was held at Hotel Cocca, on the shores of beautiful Lake Iseo (Italy). For the previous editions of this meeting of persons interested in extradition law, see eucrim 3/2018, p. 160; eucrim 3/2017, p. 118, and eucrim 3/2016, pp. 132–133. As in previous years, the 2019 conference attracted experts from many countries, including the United States, Mexico, Canada, Belarus, the England, Scotland and several countries in Continental Europe.

The seminar began with a report by UK barrister *Mark Summers* QC – who appears on a regular basis in extradition cases, including *Assange v. Sweden* in 2012 – on the current Hong Kong crisis that originated from the proposed reform to extradition arrangements.

A number of presenters offered country reports, namely on The Netherlands (by researcher *Joske Graat*), Finland (by Ministry of Justice officer *Taina Neira*), Switzerland (by lawyers *Gregoire Mangeat* and *Alice Parmentier*), Scotland (by advocate *Mungo Bovey* QC from the Faculty of Advocates of Scotland), Belarus (by lawyer *Alaksiej Michalevic*), and Poland (by lawyer *Urszula Podhalanska*). *Thomas Wahl* (an extradition expert from the Max Planck Institute for Foreign and International Criminal Law) offered an update to certain key aspects of the EAW jurisprudence in Germany and the European Court of Justice. In the 2018 edition, Wahl presented the controversial *Puigdemont* case from a German perspective; this time, we heard a presentation by *Paul Bekaert*, a Belgian lawyer, who represented Carles Puigdemont in the Belgian EAW case. Paul Bekaert also summarised the decisions of Belgian courts in other notable extradition cases when freedom of expression was at stake.

In separate sessions, *Nicola Canestrini*, a criminal lawyer from Italy, raised the question of how "free movement" rights can impact on the extradition of EU citizens to third countries while *Anna Oehmichen* (a lawyer and University lecturer from Germany) described how the abuse of the Interpol red notice (issued in the case at issue by the Dubai authorities, for a criminal offence that seems to exist only in the UAE) could lead to major violations of the fundamental rights of the requested persons. Finally, *Stefano Maffei* of the University of Parma, one of the organisers of the conference, announced the publication of his new book "*Extradition Law and Practice*", which offers an overview of the typical course of an extradition case and the description of 30 notable extradition cases.

Other participants included Canadian law student *Camille Baril;* Italian lawyer *Vanni Sancandi;* Italian graduate student *Irene Milazzo; Sibel Top*, a PhD student at the Institute of European Studies (IES) in Brussels; *Mariana Melgarejo* from the UK embassy in Mexico city; *Björn Weißenberger*, *Florian Fuchs* and *Mohammed Arjun Zahidul* (German law students) and *Kylie Zaechelein, Trenten Bilodeaux* and *Paul Borges* (from the University of the Pacific Mc George School of Law).

The Vth International Extradition Conference will be held in Northern Italy on 22–23 June 2020. All those interested should email the team of organisers at stefano.maffei@gmail.com.

whether the Member State afforded the authority a status that sufficiently guarantees independence for the issuing of EAWs. This independence is excluded if the authority is at risk of being subject to directions or instructions in a specific case from the executive. By contrast, the independence is not called into question by the fact that the Minister of Justice may issue general instructions on criminal policy. Likewise, it does not matter that the authority is responsible for conducting criminal prosecutions nor that the staff is under the direction and control of their hierarchical superiors, and thus obliged to comply with the instructions within this hierarchy. As a result, the CJEU concludes that the French public prosecutor's office – in contrast to the German one – fulfils the requirement of independence. French public prosecutors can make an independent assessment of the necessity of issuing an EAW and its proportionality, and they can exercise that power objectively.

Second, the CJEU clarified the requirement (established by the previous case law) that there must be the possibility of bringing court proceedings against the decision of the public prosecutor to issue an EAW, and these court proceedings must comply with the principle of effective judicial protection. The Luxembourg judges pointed out that the EAW system contains a two-tiered protection of the individual's procedural and fundamental rights. The protection at the first layer – the national decision on a national arrest warrant – must be supplemented by a protection as regards the issuance of the EAW (second layer). This implies that the requirements inherent in effective judicial protection must be afforded at least at one of the two layers. The establishment of a separate legal remedy against the decision to issue an EAW is only one possibility. Instead, legal orders of the EU Member States can also meet the criteria of judicial protection if the proportionality of the decision of the public prosecutor's office to issue an EAW is judicially reviewed before, or practically at the same time as that decision is adopted, or even subsequently. It is also fine if such an assessment is made in advance by the court adopting the national decision that may subsequently constitute the basis of the EAW. In conclusion, the French and Swedish systems satisfy those requirements.

➤ *The CJEU's Arguments Regarding the Belgian Public Prosecutor's Office and the EAWs Issued for Enforcing Sentences*

Regarding the specific case where the EAW was issued for the purpose of enforcing a custodial sentence imposed by a final judgment ("the Belgian case"), the CJEU found that the requirements of effective judicial protection is satisfied by the judicial review carried out by the enforceable judgment on which a subsequent EAW is based. The CJEU argued that in these cases it makes no sense to require a separate appeal against the public prosecutor's decision. The executing judicial authority can presume that the decision to issue an EAW resulted from judicial proceedings in which the requested person had all the necessary safeguards in respect of his/her fundamental rights. In addition, the CJEU points out that the FD EAW already contains a proportionality assessment because EAWs can only be issued for the purpose of enforcing custodial sentences if the sentence is at least four months.

➤ *Put in Focus*

In sum, the CJEU ruled that the French, Swedish and Belgian public prosecutor's offices satisfy the requirements for issuing an EAW.

It seems that Germany is the only EU Member State at the moment where its public prosecutor's offices are not entitled to issue EAWs following the CJEU ruling in the Joined Cases C-508/18 and C-82/19 PPU. In a judgment of 9 October 2019, the CJEU already confirmed the validity of EAWs issued by the Austrian public prosecutor (see eucrim 3/2019, p. 178). All EU Member States also replied to a questionnaire issued by Eurojust advocating that their national public prosecutor's offices are not affected by said CJEU judgment of May 2019 on the "German case" (see eucrim 2/2019, p. 110).

The question remains, however, whether the CJEU overshot the mark with its May ruling. As the German government argued in the proceedings before the Court, there had never been a single case in which the German ministries of justice issued directions or instructions towards a public prosecutor to issue or not to issue EAWs. Like in the Swedish and French system, the basis for issuing an EAW (for the purpose of prosecution) is the investigative judge's decision on whether a national arrest warrant is to be issued. It must also be questioned whether the examination of the prerequisites to issue EAWs is a routine for the national judges – more or less rubber-stamping the prosecutor's applications. In short, a rather concrete assessment of the individual cases would have been the much better approach instead of scrutinising the legal situation of independence in an abstract way.

Interestingly, the CJEU differs in its judgments of 12 December 2019 from the opinion of the Advocate General. AG *Campos Sánchez-Bordona* concluded in his opinions of 26 November 2019 that the French public prosecutor's office cannot be regarded as an "issuing judicial authority." He argued that the concept of the independence of the judicial authority implies that the public prosecutor is not subject to any hierarchical constraint or subordination. This includes not only the reception of instructions in specific cases, but also of general instructions as it is the case in the French system.

AG *Sánchez-Bordona* also advocated more stringent requirements as regards the individual's legal protection. According to his opinion, the requested person must be able to challenge the EAW issued by the public prosecutor before a judge/court in the issuing Member State, without having to wait until he is surrendered, as soon as this warrant has been issued (unless this would jeopardise the criminal proceedings) or notified to him.

Finally, the AG set out a divergent view as regards EAWs issued by the public prosecutor for the purposes of enforcing a custodial sentence. The AG required that the enforceable decision must be capable of being the subject of court proceedings similar to those that apply in the case of EAWs issued for the purpose of conducting criminal prosecution. Thus, he voiced doubts whether the Belgian system affords the necessary legal protection.

In conclusion, one cannot dismiss the impression that the judges in Luxembourg strived for mitigating the consequences of their initial ruling on the German public prosecutors by its subsequent judgments of October and December 2019 (Austrian, French, Swedish and Belgian public prosecutor's offices). The latter judgements stress more the procedural autonomy of the EU Member States since the Court acknowledged that procedural rules may vary as regards the implementation of sufficient procedural safeguards. (TW)

AG Opinion in EAW Case against Rapper: Legislation at Time of Offence Governs Interpretation of Thresholds

On 26 November 2019, Advocate General (AG) *Michal Bobek* issued his opinion in the extradition case of rapper *Valtònyc*. The CJEU has to interpret Art. 2(2) of the 2002 Framework Decision on the European Arrest Warrant (FD EAW) following a request for preliminary ruling by the Court of Appeal of Ghent, Belgium. The background of the case (C-717/18) is as follows:

In 2017, the National High Court of Spain convicted *Josep Miquel Arenas* (who performs under the name *Valtònyc*) to 3.5 years of imprisonment for rap songs that he published online in 2012 and 2013. The most severe sentence (2 years) referred to the offence of "glorification of terrorism and the humiliation of the victims of terrorism". At the time of the commitment this was the maximum sentence laid down for this offence in the Spanish Criminal Code. In 2015, however, Spain amended the offence and introduced a maximum of three years of imprisonment for "glorification of terrorism and the humiliation of the victims of terrorism." The rapper fled Spain to Belgium where he lives since 2017. In

2018, the Spanish authorities issued a European Arrest Warrant to Belgium for the purpose of executing the custodial sentence of 2017. In the EAW form, the Spanish authorities ticked the box "terrorism" with regard to the offences that gave rise to penalty. As a consequence, the double criminality requirement is not to be verified by the executing Belgian authorities in accordance with Art. 2(2) FD EAW. Art. 2(2) stipulates, however, that in these cases the offences must be punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least 3 years and as they are defined by the law of the issuing Member State.

By its reference for preliminary ruling the Ghent Court of Appeal seeks clarification which version of the Spanish criminal law is relevant in order to determine the "minimum maximum threshold" in Art. 2(2) FD EAW. Is the reference point the maximum custodial sentence applicable to the case at hand, i.e., the law that applies when the offence was committed (here: 2 years, as the offences were committed in 2012/2013)? Or is it the maximum sentence provided for by the national law in force at the time of issuing the EAW (here: 3 years following the amendment of the Spanish Criminal Code in 2015)?

AG *Bobek* clearly favours the first approach. He recommends the CJEU deciding that Art. 2(2) FD EAW refers to the criminal legislation applicable in the issuing State to the specific criminal offence(s) to which the EAW relates. In other words, it is the law actually applicable to the facts of the case to which recourse has to be made in order to assess the maximum threshold of at least three years – the precondition to dispense with the verification of double criminality. According to the AG, this conclusion results from the context of the provision and the purpose of the FD. Although the CJEU's case law is guided by the principle that an EAW can be denied only exceptionally, the AG underlines that other values, such as fundamental rights, must be respected, too. He also makes a distinction between a "structural effectiveness" of the FD and an "individual effectiveness" (effectiveness of a specific EAW in an individual case). The latter is difficult to translate into generally efficient and operational rules.

In its final remarks, the AG stresses several issues that are problematic in the case at issue, but are not subject of the questions brought to the CJEU. These issues include the significance of the fundamental right of freedom of expression in the present criminal case; the question whether the "glorification of terrorism and the humiliation of the victims of terrorism" can be subsumed under "terrorism" in the list of the 32 offences for which the verification of double criminality is excluded in the FD; and the effect of the interpretation of Art. 2(2) on Art. 2(4) FD EAW. (TW)

Financial Penalties

CJEU: No Loopholes against Enforcement of Foreign Fines

On 5 December 2019, the CJEU published an important judgment on the Framework Decision on the application of the principle of mutual recognition to financial penalties (FD 2005/214/JHA). In the case at issue (C-671/18), which was referred to the CJEU by a Polish court, the question was, among others, whether the contentious liability of persons in whose name the vehicle is registered for road traffic offences is in line with European fundamental rights. In the affirmative, this may be a reason for denying a request to recognise and execute a fine imposed in another EU country.

➤ *Facts of the Case and Legal Question on Liability:*

In the case at issue, the Dutch authorities imposed a fine of €232 against Polish national Z.P. in respect of road traffic offences in the Netherlands. Although the offences were committed by the driver of Z.P.'s vehicle and not by Z.P. personally, he can be held liable under Dutch law as the person in whose name the vehicle is registered. This form of liability is known in many European countries, whereas in others, e.g., Poland, criminal liability only lies with the individual. The referring court argued that holding somebody liable solely on the basis of information of vehicle registration data, and without any investigation being carried out, in particular in determining the actual offender, may be contrary to the principle of the presumption of innocence. Requests seeking execution of such imposed fines could then be unenforceable on the basis of Art. 20(3) of said FD.

➤ *The CJEU's Response:*

By interpreting Art. 48 of the Charter of Fundamental Rights which enshrines the principle of the presumption of innocence, the CJEU refers to the ECtHR case law concerning Art. 6(2) ECHR. The ECtHR held that the Dutch law is compatible with the presumption of innocence, in so far as a person who is fined can challenge the fine before a trial court with full competence in the matter and that, in any such proceedings, the person concerned is not left without any means of defence in that he or she can raise arguments based on Article 8 of the Netherlands Highway Code. The CJEU adds that objections against the presumption of liability of the person in whose name the vehicle is registered as laid down in the legislation of the issuing State (here: the Netherlands) are unfounded, provided that that presumption can be rebutted. Z.P. had these possibilities also in the present case.

The CJEU pointed out that FD 2005/214 is intended to establish an effective mechanism for cross-border recognition and execution of final decisions imposing financial penalties. Grounds for refusal to recognise or enforce such decisions must be interpreted restrictively.

➤ *Infringements of Defence Rights?*

Regarding a second set of questions of whether Z.P. had effective defence

rights, the CJEU noted that the person concerned must have had sufficient time to contest the decision in question and to prepare his defence, and was in fact provided with the decision imposing the financial penalty. It is in line with the FD and the Charter right to an effective legal remedy if the decision was notified to the person concerned in accordance with the legislation of the issuing state. The CJEU also held a period of six weeks as time limit for exercising the right of appeal (starting with the date of decision) sufficient to guarantee the person's defence rights.

➤ *Put in Focus:*

The CJEU confirms its case law established in other mutual recognition instruments that grounds for refusal are to interpreted in a very restrictive way. Denial of requests can only be the exception, also when fundamental rights infringements may be at stake. In the present judgment on financial penalties, the CJEU also concludes that the law of the issuing state on liability of persons prevails over potentially differing laws of other EU Member States. Therefore, the judgment has not only an impact to Poland, but also to other EU countries for which liability of persons who did actually not commit an offence is alien. (TW)

Law Enforcement Cooperation

EU Digital Evidence Situation Report

spot light

On 20 December 2019, Europol published a new report, giving an overview on the status of access of EU Member States to electronic evidence held by foreign-based Online Service Providers (OSPs) in the context of criminal investigations. Looking at the year 2018, the new EU Digital Evidence Situation Report (SIRIUS) looks at the volume of requests from EU Member States to OSPs, the main reasons for refusal or delay of EU requests, and the main challenges in the process.

According to the report, over 74% of EU law enforcement requests to the eight major OSPs in 2018 originated in three EU Member States: Germany, France, and the UK. The three OSPs most frequently requested were Facebook (30%), Google (26%), and Apple (24%). The overall success rate of requests to major OSPs in 2018 was calculated at 66%. The most frequently needed type of data in the majority of investigations appeared to be traffic data (e.g., connection logs, IP addresses, number of messages), followed by basic subscriber information (e.g., name, e-mail, phone number), and content data (e.g., photos, mail/message content, files).

Looking at issues encountered by EU law enforcement, with requesting data from OSPs, the main problems identified by the report are the lengthy MLA proceedings, the lack of standardized company procedures when receiving requests from EU law enforcement, and how to determine the type of data held by companies. Further issues outlined in the report include the short data retention period, the lack of timely response in urgent cases, and the non-standardization of OSP policies.

Reasons for refusal or delay in processing direct requests, as given by the OSPs, include wrong identifiers, overly broad requests, requests concerning non-existing data or data requiring judicial cooperation, the lack of reference to Valid Legal Basis (VLB) under the domestic legislation of the requesting authority, the wrong legal entity of the OSP being addressed, and the lack of requests for preservation. Other challenges faced by the OSPs are language barriers, how to ensure the authenticity of received documents, and misunderstandings caused by little or no previous knowledge on the part of requesters of OSP services and products.

The report provides for several recommendations to both the OSPs and EU law enforcement agencies. OSPs are asked to provide clear guidelines for law enforcement authorities, including information about which data sets can be requested and to which legal entity the data requests should be addressed; to prepare periodic transparency reports on requests from EU authorities, including standardized data categories across OSPs and files in CSV formats; and to clearly inform the requesting authority of the reasons for rejection without delay. EU law enforcement agencies are asked to provide periodic trainings to officers dealing with cross-border requests to OSPs; to establish Points of Single Contact (PSCs) within the law enforcement agency to deal with the most relevant OSPs; and to collect statistics on cross-border requests to OSPs.

The report is an outcome of the SIRIUS project, which was launched by Europol in October 2017. The project was initiated in response to the increasing need of the EU law enforcement community to access electronic evidence for internet-based investigations. More than half of all criminal investigations today include a cross-border request to access e-evidence (such as texts, e-mails, or messaging apps). The SIRIUS project is spearheaded by Europol's European Counter-Terrorism Centre and European Cybercrime Centre, in close partnership with Eurojust and the European Judicial Network. It aims to help investigators cope with the complexity and volume of information in a rapidly changing online environment, by providing guidelines on specific OSPs and investigative tools. Europol established a platform for experts (restricted access) by means of which the multidisciplinary SIRIUS community can have access to a wide range of resources.

The EU Digital Evidence Situation Report provides empirical information on e-evidence in a systematic and comprehensive way for the first time. It not only includes information from all EU Member States but also comprises data from both judicial and police authorities. Another added value is the input by 12 OSPs (mainly based in the USA, e.g.,

Airbnb, Facebook, Google, Microsoft, Twitter). The report is sure to influence discussion on the establishment of a new legal framework on e-evidence at the EU level (see, recently, eucrim 3/2019, pp. 179 et seq. with further references) (CR)

Commission Updates on E-Evidence Negotiations with US and at Council of Europe

At the JHA Council meeting of 2–3 December 2019, the Commission updated the Council on the state of play of the negotiations for an EU-US agreement on cross-border access to e-evidence, on the one hand, and on a second additional Protocol to the Budapest Convention, on the other hand. The Council gave green light for both negotiations when it endorsed the respective mandates in June 2019 (see eucrim 2/2019, p. 113). Regarding the EU-US agreement, three meetings took place (September, November, and December 2019), where the parties mainly stated their starting negotiating positions.

Negotiations on the second protocol to the Budapest Convention on Cybercrime advanced at the Council of Europe, but several important topics have still to be addressed.

Both the EU-US agreement and the protocol to the Budapest Convention are designed to complete the respective EU regime on e-evidence which is currently negotiated between the European Parliament and the Council (see eucrim 3/2019, pp. 181 et seq.). The new legal frameworks are to facilitate access to electronically stored data that is needed for prosecuting crimes. It would establish new forms of assistance, in particular by enabling law enforcement authorities to directly request private IT service providers to hand over the data. For further information about the ongoing developments in the field of e-evidence, see also eucrim 3/2019, pp. 179 et seq., eucrim 2/2019, pp. 113 et seq., and eucrim 1/2019, pp. 38 et. seq. with further references. (TW)

Meeting of EU Justice and Home Affairs Agencies

On 22 November 2019, the heads of the nine EU Justice and Home Affairs (JHA) agencies met at Europol's headquarters in The Hague. The topics of discussion were as follows:

- Implementation of the New Strategic Agenda 2019–2024;
- State-of-play of the interoperability project;
- Common efforts in reinforcing diversity and inclusion in the workplace.

As a result of the meeting, the agencies' representatives signed a common statement to highlight the importance of inclusive corporate culture and strong diversity and to ensure equal opportunities for all staff members while embracing their diversity.

The following nine agencies are members of the JHA Agencies Network:

- European Asylum Support Office (EASO);
- European Border and Coast Guard Agency (Frontex);
- European Institute for Gender Equality (EIGE);
- European Monitoring Centre for Drugs and Drug Addiction (EMCDDA);
- European Union Agency for Fundamental Rights (FRA);
- European Union Agency for Law Enforcement Cooperation (Europol);
- European Union Agency for Law Enforcement Training (CEPOL);
- European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA);
- European Union Judicial Cooperation Unit (EUROJUST). (CR)

Council of Europe*

Reported by Dr. András Csúri (AC)

Specific Areas of Crime

Corruption

GRECO and FEDE Launch New Anti-Corruption Education Module

On 20 December 2019, GRECO and the Federation for Education in Europe (FEDE), an international NGO having participatory status with the CoE, presented an education module on anti-corruption for the 2019–2020 academic year. The module includes summary sheets, takeaway messages, and test questions. It will be part of FEDE's course on European Culture and Citizenship, reaching out to over 10,000 school students annually. An overview is provided in factsheets. The main focus is on the definition, forms, and cartography of corruption as well as its causes and how to fight it.

GRECO: *Ad hoc* Report on Greece

On 18 December 2019, GRECO published an *ad hoc* report on Greece. In the past, GRECO, together with the Or-

* If not stated otherwise, the news reported in the following sections cover the period 16 November – 31 December 2019.