News

Actualités / Kurzmeldungen

European Union*

Reported by Thomas Wahl (TW), Cornelia Riehle (CR), and Christine Götz (CG)

Foundations

Fundamental Rights

10th Anniversary of Charter: Council Conclusions

On the occasion of the 10th anniversary of the Charter of Fundamental Rights, the JHA Council adopted conclusions on the Charter, their state of play, and future work. At its meeting on 7 October 2019, the ministers of justice of the EU Member States reaffirmed that the Union is based on common values, as enshrined in Art. 2 TEU, which is founded on respect for human dignity, freedom, democracy, equality, the rule of law, and respect for human rights, including the rights of persons belonging to minorities. These rights are a cornerstone of the European Union and must be fully respected by all Member States and EU institutions. At the meeting, the ministers also reaffirmed the commitment to the EU's accession to the ECHR (see separate news item).

Taking note of the Commission report on the application of the Charter and the FRA fundamental rights report (see eucrim 2/2019, p. 82), the Council acknowledges that challenges persist, particularly in the area of non-discrimination, and that the fight against all forms of discrimination must continue.

Another problem is the public's low awareness of the Charter. The Council calls on Member States to strengthen their awareness-raising and training activities towards all key stakeholders, including policymakers, civil servants, legal practitioners as well as national human rights institutions, civil society organisations, etc. The e-justice portal is considered to be an important tool supporting this endeavour. Thematic discussions and the annual exchange of views on application of the Charter at the national level should also be promoted.

The Commission is to ensure the consistency of legislative and policy initiatives with the Charter and to further enhance fundamental rights impact assessments for all relevant legislative proposals.

While welcoming the Fundamental Rights Agency's Charter-related work – including awareness raising, e-tools, and training as well as expertise and data that are useful for the preparation of initiatives –, the Council stressed that it will "consider carefully" any proposal on increasing the Agency's legal clarity and efficiency.

Ultimately, the conclusions recognise the essential role of civil society organisations in promoting fundamental rights. The Council emphasizes that Member States must refrain from any unnecessary, unlawful, or arbitrary restrictions on civil society. It also points out that transparent, sufficient, and easily accessible funding is crucial for civil society organisations. (TW)

Council: EU Should Accede to ECHR

At their Council meeting on 7 October 2019, the ministers of justice of the EU Member States reaffirmed the EU's commitment to acceding to the European Convention on Human Rights (ECHR). The ministers also agreed to supplementary negotiating directives. They will be addressed to the Commission so that it can resume negotiations with the Council of Europe in the near future. They will take into account the objections raised by the Court of Justice, which found a draft agreement negotiated in 2013 to be incompatible with the treaties of the European Union (Opinion 2/13 of 18 December 2014).

In May 2019, the Commission submitted an analysis on the legal issues of the CJEU's decision, which formed the basis for the adapted negotiation guidelines. It is expected that the Commission will resume the negotiations soon. The

* If not stated otherwise, the news reported in the following sections cover the period 1 August – 15 November 2019.

Treaty on European Union provides for the accession of the EU to the ECHR. Its objective is to reinforce the common values of the Union, improve the effectiveness of EU law, and enhance the coherence of fundamental rights protection in Europe. (TW)

Council Updates EU Guidelines Against Torture and Ill-Treatment

On 16 September 2019, the Council adopted revised Guidelines on EU policy towards third countries on torture and other cruel, inhuman, or degrading treatment or punishment.

The purpose of the Guidelines is to provide practical guidance to EU institutions and Member States, which can be used in their engagement with third countries and in multilateral human rights fora, in order to support ongoing efforts to eradicate torture and other ill-treatment worldwide. They complement other instruments of the EU's human rights policy, e.g., the EU's Strategic Framework on Human Rights and Democracy with its Action Plan on Human Rights and Democracy, the EU's policy framework on support to transitional justice, and the Guidelines on promoting compliance with International Humanitarian Law.

The Guidelines set out various policy tools as well as operational measures to support third countries in their prohibition and prevention of torture and ill-treatment. (TW).

CJEU Rules on Independence of Poland's Disciplinary Chamber of the Supreme Court

In its judgment of 19 November 2019, the Grand Chamber of the CJEU established criteria under which the new Disciplinary Chamber of the Polish Supreme Court can be considered independent and impartial. The judgment is based on a reference for a preliminary ruling brought by the Labour and Social Insurance Chamber of the Polish Supreme Court (Joined Cases C-585/18, C-624/18, and C-625/18).

In the cases at issue, Supreme Court judges protested against their early retirement, following the new Polish legislation lowering the retirement age of Supreme Court judges (see also case C-619/18 and the CJEU's judgment of 24 June 2019 in this case in eucrim 2/2019, p. 80). A new Disciplinary Chamber at the Supreme Court was established to hear such actions by a new 2017 law. The referring court, before which such actions were heard prior to the reform, calls into question whether the Disciplinary Chamber offers sufficient guarantees of independence under Union law and whether it can eventually disapply national legislation that transferred competence to the Disciplinary Chamber (for details about the case and the opinion of AG *Tanchev*, see eucrim 2/2019, p. 81).

The judges in Luxembourg first had to deal with several objections against the admissibility of the reference and rejected the arguments put forward by the Polish Public Prosecutor General, *inter alia,* as follows:

- Arg.: Laying down rules on the jurisdiction of national courts and national councils falls within the exclusive competence of Member States. ↔ As the CJEU has previously held, although the organisation of justice in the Member States falls within their competence, they are required to comply with their obligations deriving from EU law when exercising that competence.
- Arg.: The provisions of national law at issue do not implement EU law or fall within its scope and therefore cannot be assessed under that law (especially Art. 19 para. 1 subpara. 2 TEU and Art. 47 of the Charter). ↔ The applicants in the main proceedings are relying on the prohibition against discrimination in employment provided for by Directive 2000/78; thus, a situation is given in which the Member State "implements EU law" in the sense of Art. 51(1) of the Charter. In addition, Art. 19 TEU does not require that Member States be implementing EU law.
- Arg.: The CJEU is not allowed to interpret the Charter because it has to respect Protocol No. 30 on application of the Charter of Fundamental Rights of the European Union to the Republic of Poland and to the United Kingdom. ↔ The protocol does not concern the second subparagraph of Art.19(1) TEU, and it neither calls into question the applicability of the Charter in Poland, nor is it intended to exempt the Republic of Poland from its obligation to comply with the provisions of the Charter.
- Arg.: The reference is no longer necessary because the referring Labour and Social Insurance Chamber disregards the new composition and jurisdiction of the Polish courts. ↔ The arguments put forward concern matters of substance and cannot affect the admissibility of the questions referred.

As regards the substance of the questions, the CJEU reaffirmed that the Polish disciplinary regime must comply with the right to effective judicial protection as enshrined in Article 47 of the Charter. This means, in particular, that everyone is entitled to a fair hearing by an independent and impartial tribunal. The CJEU then reiterated its settled case law on the requirement that courts be independent:

- External dimension: The court concerned can exercise its functions entirely autonomously, without being subject to any hierarchical constraint or subordinated to any other body and without taking orders or instructions from any source whatsoever, thus being protected against external interventions or pressure liable to impair the independent judgment of its members and to influence their decisions;
- Internal dimension (linked to impartiality): An equal distance is maintained from the parties to the proceedings and their respective interests with regard to the subject matter of those proceedings. This aspect requires objectivity and the absence of any interest in the outcome of the proceedings apart from the strict application of the rule of law;

- Any guarantees of independence and impartiality require rules, particularly as regards the composition of the body, and the appointment, length of service, and grounds for abstention, rejection, and dismissal of its members, in order to dispel any reasonable doubt in the minds of individuals as to the imperviousness of that body to external factors and as to its neutrality with respect to the interests before it;
- In accordance with the principle of the separation of powers, which characterises the operation of the rule of law, the independence of the judiciary must be ensured in relation to the legislature and the executive;
- Organisational and procedural rules must be such as to preclude not only any direct influence, in the form of instructions, but also any more indirect forms of influence.

The CJEU concluded that it is up to the referring court to ascertain whether the framework of the new Disciplinary Chamber fulfills these requirements, but it provides several suggestions as to which specific factors should be considered:

For example, the mere fact that the judges of the Disciplinary Chamber were appointed by the President of the Republic of Poland does not infringe impartiality *if*, once appointed, they are free from influence or pressure when carrying out their role. The prior participation of the National Council of the Judiciary, which is responsible for proposing judicial appointments, would be acceptable *if* that body is itself sufficiently independent of the legislature, the executive, and the President of the Republic.

Furthermore, factors that characterise the Disciplinary Chamber more directly must also be taken into account, such as its exclusive jurisdiction, its constitution with newly appointed judges alone, and its high degree of autonomy within the Supreme Court.

Altogether, the judges in Luxembourg highlighted that, although any single factor is not capable of calling into question the independence of the Disciplinary Chamber per se and seen in isolation, this may conversely not be true once the factors are viewed together.

Ultimately, the Grand Chamber of the CJEU examined the legal consequences that occur if the referring court negates the independence of the Disciplinary Chamber, and concluded: "If that is the case, the principle of the primacy of EU law must be interpreted as requiring the referring court to disapply the provision of national law which reserves jurisdiction to hear and rule on the cases in the main proceedings to the abovementioned chamber, so that those cases may be examined by a court which meets the abovementioned requirements of independence and impartiality and which, were it not for that provision, would have jurisdiction in the relevant field."

New Polish regulations on the disciplinary regime against judges are also the subject of infringement proceedings initiated by the Commission (Case C-791/19; see also eucrim 2/2019, pp. 81–82). In previous judgments, the CJEU had already declared the lowering of the retirement age for judges at the Supreme Court and at the level of ordinary courts to be incompatible with Union law. (TW)

CJEU: Polish Retirement Rules at Ordinary Court Level Contrary to EU Law

On 5 November 2019, the Grand Chamber of the CJEU declared that another issue of the Polish justice reform was not in line with EU law. After having ruled on 24 June 2019 that lowering the retirement age of the Supreme Court judges is contrary to EU law (see Case C-619/18 in eucrim 2/2018, p. 80), the CJEU also affirmed non-compliance with regard to the new retirement scheme for Polish judges and public prosecutors (Case C-192/18).

A Polish law of 12 July 2017 lowered the retirement age of ordinary court judges and public prosecutors as well as the age for early retirement of Supreme Court judges to 60 years for women and 65 years for men (previously 67 for both sexes). The power of the Polish Minister of Justice to extend the active service period of judges at the ordinary courts above and beyond the new retirement age was also the subject of the case. Since the European Commission found these rules to be contrary to EU law, it brought an action for failure to fulfil obligations before the Luxembourg Court.

The CJEU first held that the differences in retirement age between female and male judges/prosecutors is a direct discrimination based on sex. The CJEU rejected the argument Polish government that the difference is an "authorised positive action" under Article 157(4) TFEU and Article 3 of Directive 2006/54, because early retirement for women would indirectly compensate them for difficulties experienced in receiving promotions throughout their professional careers. The CJEU held on the contrary that "(t)he setting, for retirement, of an age condition that differs according to sex does not offset the disadvantages to which the careers of female public servants are exposed by helping those women in their professional life and by providing a remedy for the problems which they may encounter in the course of their professional career." As a result, the new legislation infringes Art. 157 TFEU (principle of equal pay for male and female workers for equal work) and Directive 2006/54 (implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation).

Second, the CJEU also held that the discretion given to the Minister of Justice to decide whether or not to authorise that ordinary court judges may continue to carry out their duties above and beyond the new (lower) retirement age is contrary to Union law. It found that the substantive conditions and detailed procedural rules governing that decision-making power are contrary to the criteria for independence of judges, which can

be deduced from Art. 19 para. 1 subpara. 2 TEU and as set out in the first judgment on the Polish justice reform of 24 June 2019. The too vague and unverifiable conditions for extension and the potential length for the discretionary decision are not acceptable.

Moreover, the judges in Luxembourg found that the necessary imperviousness of judges to all external intervention or pressure is not guaranteed. They mainly argue that the combination of lowering the normal retirement age of judges at the ordinary courts and of conferring discretion for extension to the Minister of Justice fails to comply with the principle of irremovability. In this context, the judges remarked that "the combination of the two measures … is such as to create, in the minds of individuals, reasonable doubts regarding the fact that the new system might actually have been intended to enable the Minister for Justice, acting in his discretion, to remove, once the newly set normal retirement age was reached, certain groups of judges serving in the ordinary Polish courts while retaining others of those judges in post."

In sum, the CJEU follows the conclusion of AG *Tranchev* of 20 June 2019 (see eucrim 2/2019, pp. 80–81) and its judgment of 24 June 2019 on changes to the retirement age of Supreme Court judges (see above). It is the second of a series of pending cases before the CJEU that attack the justice reform in Poland for exerting more political influence into the judiciary. (TW)

AG: References Against Disciplinary Proceedings Against Polish Judges at Ordinary Courts Inadmissible

On 24 September 2019, Advocate General *Tanchev* proposed that references for a preliminary ruling of two Polish district courts voicing doubt as to the compatibility of the new disciplinary regime introduced in Poland via judicial reforms in 2017 with Art. 19(1) subpara. 1 TEU should be declared inadmissible.

The cases are registered as Joined Cases C-558/18 and C-563/18 (*Miasto Łowicz v Skarb Państwa – Wojewoda Łódzki, joined parties: Prokuratura Regionalnaw Łodzi, Rzecznik Praw Obywatelskich* and *Prokuratura Okręgowa w Płocku v VX, WW, XV)*.

The cases at issue refer first to a civil law suit between the municipality of Łowicz and the State Treasury before the District Court of Łódź, and, second, to a criminal trial before the District Court of Warsaw against a gang whose defendants seek protection from the state because of their cooperation with the law enforcement authorities. Both district courts submit that they may take decisions that are not in favour of the State authorities; therefore they fear becoming the subject of disciplinary proceedings. The referring judges are concerned that the disciplinary regime introduced in Poland in 2017 may entail politically motivated disciplinary penalties, which infringes the second subparagraph of Art. 19(1) TEU.

AG *Tanchev* first affirmed that the situation in the main proceedings falls within the material scope of Art. 19(1) subpara. 2 TEU (the obligation for Member States to provide remedies sufficient to ensure effective legal protection in the fields covered by Union law). Accordingly, the CJEU is vested with the authority "to rule on structural breaches of the guarantees of judicial independence, given that Article 19 TEU is a concrete manifestation of the rule of law, one of the fundamental values on which the European Union is founded under Article 2 TEU." Structural breaches of judicial independence inevitably impact on the preliminary ruling mechanism under Art. 267 TFEU and thus on the capacity of Member State courts to act as EU Courts.

However, AG *Tanchev* found that requirements on admissibility for a preliminary ruling have not been met in the present case. The reference does not sufficiently explain the relationship between the relevant provisions of EU law and the Polish measures in question. Furthermore, the AG observed that there seems to be mere subjective fear on the part of the referring court, because concrete disciplinary proceedings have not yet been initiated. Therefore, the questions remain hypothetical as to what makes the request inadmissible under Art. 267 TFEU.

The reference at issue is one of a series of proceedings before the CJEU in which Polish judges are taking a stand against the judicial reforms in Poland, which attack the rule of law. In total, they have brought forward around 14 references for preliminary rulings. In addition to these references, the Commission initiated infringement proceedings (see, *inter alia*, Case C-619/18 and Case C-192/18 on the lowering of the retirement rules for judges and public prosecutors – all reported in eucrim 2/2019, pp. 80 ff. and in this issue). In the Joined Cases C585/18, C-624/18 and C-625/18, by judgment of 19 November 2019, the CJEU ruled on the independence of the Polish Disciplinary Chamber in cases involving Supreme Court judges taking legal action against their early retirement. (TW)

Commission Refers New Disciplinary Regime for Polish Judges to CJEU

After Poland failed to address the Commission's concerns about the new disciplinary regime for Polish judges, set out in the reasoned Opinion of the Commission of 17 July 2019 (see eucrim 2/2019, pp. 81–82), the Commission referred the case to the European Court of Justice on 10 October 2019. The Commission is mainly critical of the following issues:

- The possibility to initiate disciplinary investigations and sanctions against ordinary court judges is based on the content of their judicial decisions, including exercise of their right under Art. 267 TFEU to request preliminary rulings from the CJEU;
- The new Disciplinary Chamber of the Polish Supreme Court does not guarantee independence and impartiality in the

composition and selection process, as required by EU law and CJEU case law;
- The President of the Disciplinary Chamber has almost unfettered discretion to determine the disciplinary court of first instance, so that the principle that a court is "established by law" is not respected;
- There are no guarantees that disciplinary proceedings against judges are processed within a reasonable timeframe;
- The judges' defence rights are undermined.

The case is registered at the CJEU as C-791/19. The Commission applied for an expedited procedure, which is also in line with its new concept to strengthen the rule of law, as presented in the Commission Communication of 17 July 2019 (see eucrim 2/2019, p. 79).

The new disciplinary regime against Polish judges of ordinary courts is also subject to a reference for preliminary ruling (Joined Cases C-558/18 and C-563/18). On 24 September 2019, AG *Tanchev* proposed declaring these references inadmissible; they were brought to the CJEU by two Polish district courts. Other reforms of the Polish judicial system that were introduced by Poland two years ago and that seek to increase political influence in the justice sector will keep the CJEU busy, since they are subject to other infringement proceedings and references for preliminary rulings. In total, Polish courts have made references for preliminary rulings in about 14 cases. On 19 November 2019, the Grand Chamber of the CJEU already indicated that the new Disciplinary Chamber of the Supreme Court, which is responsible for deciding complaints by Supreme Court judges, may infringe the guarantees of independence and impartiality. On 24 June 2019, the CJEU ruled that the Polish reform lowering the retirement age of Supreme Court judges is contrary to EU law (Case C-619/18, see eucrim 2/2019, p. 80). On 5 November 2019, the CJEU declared that the new retirement scheme for Polish judges and public prosecutors at the ordinary court level is not in line with EU law. (TW)

Hungary and Poland Impede Conclusions on Rule-of-Law Evaluation

Hungary and Poland blocked the adoption of Council conclusions on evaluation of the rule-of-law dialogue. The rule-of-law dialogue was established in 2014. It consists of a structured dialogue between the Commission and Member States that disrespect the rule of law and the Annual Dialogues on the Rule of Law, allowing national governments to discuss rule-of-law related issues within the Council. In 2016, the General Affairs Council agreed to reevaluate the framework by the end of 2019.

At its meeting on 19 November 2019, the General Affairs Council discussed the evaluation and the draft conclusions. Ministers also exchanged views with FRA Director, Michael O'Flaherty. The Finnish Presidency stated that 26 delegations supported the conclusions as published in Council Document 14173/19. They advocate a yearly stocktaking exercise revolving around the state of play and key developments in the rule of law. Such an annual stocktaking could draw on the Commission's annual rule-of-law reports, which would in turn create synergies between the institutions. Furthermore, ministers wish "for the dialogue to be stronger, more result-oriented and better structured, for preparations for the dialogue to be more systematic, and for proper follow-up to be ensured." The organisation and in-depth discussion of rule-of-law-related issues in other Council configurations is also encouraged.

Strengthening the rule of law is one of the top priorities of Finland's Council Presidency during the second half of 2019. The Finnish Presidency welcomed the Commission's new concept to strengthen the rule of law, as presented on 17 July 2019 (see eucrim 2/2019, p. 79). It also supports the proposal by Belgium and Germany for a periodic peer review mechanism on the rule of law, which could reinforce mutual understanding and unity among the EU Member States. (TW)

Area of Freedom, Security and Justice

New Eurobarometer: Strong Increase in Citizens' Positive Perception of the EU

A new Eurobarometer survey was released on 5 August 2019. It shows a strong general increase in citizens' positive perception of the European Union. The survey was conducted by means of 27,464 face-to-face interviews in the 28 Member States and five candidate countries in June 2019, shortly after the European elections.

According to the survey, trust in the EU is at his highest level since 2014 and remains higher than trust in national governments or parliaments. Trust in the EU increased in 20 Member States, with the highest scores in Lithuania (72%), Denmark (68%) and Estonia (60%).

Support for the Economic and Monetary Union with one single currency, the euro, has reached a new record high within the Eurozone. Throughout the EU, support for the euro has not changed since the last survey in autumn 2018 and remains at its highest level since spring 2007.

Across the EU, 73% of citizens feel they are citizens of the EU. In all 28 Member States, the majority of respondents feels this way (the national scores range from 93% in Luxembourg to 52% in Bulgaria).

Immigration is still seen as the main concern at the EU level, even though the number of respondents mentioning this concern has decreased since autumn 2018. The survey is marked by a significant rise in concern over climate change and the environment. Climate change, which was ranked fifth in autumn 2018, now ranks second as an issue for the first time. The concern over terrorism, which

New LLM Programme "European Criminal Justice in a Global Context" at Utrecht University

In the next academic year, the Utrecht Law School is starting a new master LLM programme. The programme focuses on the role of criminal justice systems in a Europeanized and internationalized legal environment, including enforcement and applicable human rights and constitutional standards. The content focuses on the following:

- The constitutional foundations for criminal justice in a Europeanized setting, including the fundamental rights dimension and the harmonisation of defence rights and safeguards;
- The effects and impact of EU law on domestic criminal justice and its relationship with administrative law enforcement in such areas as anti-money laundering, financial fraud, and other serious cross-border offences;
- The different legal regimes for transnational enforcement cooperation and the exchange of information, including the European Arrest Warrant and the European Investigation Order;
- The relationships between national criminal justice and EU authorities such as Eurojust and the European Public Prosecutor's Office;
- The relationship between European criminal justice and its global context (external dimension).

For details about the programme, its objectives, career prospects, admission and application procedures, etc., visit the website on the master programme. (TW)

was ranked first in spring 2017, has once again slightly decreased since autumn 2018 and is now ranked third, together with concerns about the economic situation and the state of Member States' public finances. 9% of the respondents mention crime as one of their two main concerns (tenth rank). The number of people mentioning concern about crime has remained fairly stable, between 9 and 10%, since spring 2017. (CG)

Security Union

20th Progress Report on Security Union

spot light

The EU achieved progress in fighting terrorism, stepping up information exchange, countering radicalisation, preventing violent extremism, and addressing cybersecurity; however, further efforts are needed. This is the main message of the "20th progress report towards an effective and genuine Security Union" that was presented by the European Commission on 30 October 2019. The report reveals that, since the attacks in Halle/Germany and in Paris/France at the beginning of October 2019, both right-wing extremism/anti-Semitism and jihadi inspired terrorism continue to be security priorities in the EU.

Within the framework of the report series (for the 19th progress report, see eucrim 2/2019, p. 82), the 20th progress report focuses particularly on the following:

- Cybersecurity of 5G networks;
- Countering disinformation;
- External dimension of cooperation in the Security Union.

In the field of *legislative priorities*, the report highlights the following issues:

- In order to prevent radicalisation (both jihadi and right-wing violent extremism), the legislative proposal to prevent the dissemination of terrorist content online is considered essential. According to the Commission, this legislation would set clear rules and safeguards obliging internet platforms to take down terrorist content within one hour upon receipt of a reasoned request by competent authorities and to take proactive measures (for the proposal, see eucrim 2/2018, pp. 97–98 and the article by *G. Robinson*, eucrim 4/2018, p. 234). The European Commission calls on the legislators (Council and EP) to swiftly conclude negotiations by the end of 2019.
- Within the framework of the EU Internet Forum, internet companies agreed on their commitment to the EU Crisis Protocol – an enhanced cooperation mechanism ensuring coordinated and rapid reaction to contain the spread of viral terrorist or violent extremist content online;
- Implementation of interoperability of the systems for security and border/migration control is one of the top priorities for the Commission in 2020. The report points out the necessity of stronger and smarter information exchange. However, further legislation to complete established legislation on interoperability (see eucrim 2/2019, pp. 103–104) is needed. Therefore, the EP and Council are called on to swiftly reach agreement on the pending proposals on technical amendments to ETIAS and the reforms of the Visa Information System and Eurodac;
- While welcoming the launch of the European Judicial Counter Terrorism Register at Eurojust (see eucrim 2/2019, p. 100), the Commission calls on the EP to quickly advance the legislative proposal of law enforcement access to e-evidence (see, in this context, the latest news in the category "Law Enforcement Cooperation");
- Cybersecurity remains a key area of EU action. In this context, the report points to the EU cybersecurity certification framework (see eucrim 2/2019, p. 98), which now needs to be implemented. The legislative initiative for a European Cybersecurity Industrial, Technology and Research Competence and Network of National Coordination Centres, however, is still pending and should be concluded soon. In addition, work continuous on tackling hybrid threats. This includes the elaboration of a "conceptual model" framework to support Member States in identifying the

type of hybrid attack they might face. For hybrid threats on the EU agenda, see also eucrim 2/2019, p. 85.

Cybersecurity and resilience of 5G networks is another hot topic where EU action is required in the near future. The progress report highlights the risk assessment report by the Member States (with the support of the European Commission and the European Agency for Cybersecurity) published on 9 October 2019. The report identifies a number of important cybersecurity challenges for 5G that authorities, suppliers, and users are likely to face in the future. The report reveals that suppliers will be the focus of cyberattacks, in particular those from non-EU countries. The Commission calls on Member States to swiftly agree on a toolbox of mitigating measures to address the identified cybersecurity risks at the national and Union levels, as recommended by the Commission in March 2019.

The Commission also takes stock of the progress made in *countering disinformation* and in protecting elections against other cyber-enabled threats. The Commission, *inter alia*, evaluated the Code of Practice on Disinformation for online platforms and the advertising sector that became applicable in October 2018. It acknowledges efforts made by the signatories; however, more consistent actions are necessary because actions taken by the platforms vary in terms of speed and scope in order to ensure the implementation of their commitments.

As in previous reports, the Commission is not satisfied with the *implementation of core EU legislation* in the fields of terrorism and cybercrime. The Commission urges Member States to fully transpose, *inter alia*, the following EU legislation:

- The EU Passenger Name Record Directive;
- The Directive on combating terrorism;
- The Directive on control of the acquisition and possession of weapons;
- The 4th Anti-Money Laundering Directive.

Ultimately, the report provides updates on the *external dimension of the EU's security policy*. It highlights the proposed opening of negotiations for an agreement allowing the exchange of personal data between Europol and the New Zealand authorities to fight serious crime and terrorism. New Zealand has been added to the list of priority countries for such agreements; negotiations with eight other priority countries from the Middle East/North Africa (MENA) region are ongoing.

Alongside the Europol cooperation with third countries, another cornerstone is the transfer of passenger name record data (PNR). The Commission points out its recommendation to the Council to authorise negotiations for an EU-Japan PNR agreement. It is envisaged that arrangements be in place before the start of the Olympic games in Tokio in 2020. Negotiations with Canada on a new PNR agreement are on track. On the international level, the Commission presented a proposal to the Council for a decision on the EU position in the International Aviation Organization with regard to standards and recommended practices on passenger name record data.

Security cooperation with the Western Balkans remains at the top of the EU agenda. In this context, the progress report refers to the bilateral anti-terrorism arrangements with Albania and North Macedonia, which were signed on 9 October 2019 and which implement the 2018 Joint Action Plan on Counter-Terrorism for the Western Balkans. The arrangements include tailor-made, concrete priority actions which the countries should take in the course of 2019 and 2020, and set out the Commission's support in this regard. In addition, the Commission signed an agreement with Montenegro on border management cooperation between Montenegro and the European Border and Coast Guard Agency.

In conclusion, the 20th progress report on the Security Union states that, besides the need for the swift conclusion of pending legislative proposals, agreed measures and instruments must "be turned into an operational reality on the ground" in the EU Member States. (TW)

Self-Assessment Reports on EU Code of Practice on Disinformation

In October 2018, the industry agreed on a self-regulatory EU Code of Practice to address the spread of online disinformation and fake news. The signatories recognised the objectives outlined in the Commission Communication "Tackling online disinformation – a European approach" of April 2018. This was the first worldwide "private-public partnership" to fight disinformation. The Code of Practice is also one of the main pillars of the EU's Action Plan against the phenomenon of disinformation and fake news.

The Code has been signed by the leading IT companies Facebook, Google, Twitter, Mozilla, and Microsoft as well as seven European trade associations. They commit themselves to deploy policies and processes in relation to the scrutiny of ad placements, political advertising and issue-based advertising, integrity of services and the empowerment of consumers, and the research community. An annual account report from each company/association forms the basis for measuring and monitoring the Code's effectiveness.

These annual self-assessment reports were published on 29 October 2019. In addition, the Commission published a summary and brief analysis of the reports.

The Commission acknowledges that the signatories have made comprehensive efforts to fulfil their commitments over the last 12 months. The Code led to higher transparency regarding the platform's policies against disinformation and the ability to monitor structured dialogues. However, further serious steps by individual signatories and the community as a whole are still necessary.

The Commission observes that the reported actions taken by the platforms vary significantly in terms of scope and speed. In general, actions to empower consumers and the research community lag behind the original commitments (as evidenced prior to the European Parliament elections in May 2019). Furthermore, there are differences across the Member States as regards the deployment of the respective policies for the various commitments included in the Code.

Although cooperation between the platforms and stakeholders (e.g., fact-checkers, researchers, and civil organisations) improved, the provision of data and search tools is still episodic and arbitrary and does not respond to the demands of researchers for independent scrutiny. More efforts are also needed to establish sound cooperation with truly independent organisations.

The Commission observed that the platforms provided information on EU-specific metrics regarding the implementation of the Code; however, these metrics mainly focus on the number of accounts taken down or ads rejected. They do not enable a qualitative insight into the actual impact of the self-regulatory measures and mechanisms for independent scrutiny.

Lastly, the Commission notes that other IT platforms and advertising companies/services operating in the EU have not joined the Code.

The self-assessment reports are the starting point for a comprehensive assessment of the Code's effectiveness, which will be carried out by the Commission itself. The assessment is expected for the first half of 2020. The Commission will additionally take the following into account:

- Input from the European Regulators Group for Audiovisual Services (ERGA), as foreseen in the Action Plan against Disinformation;
- An evaluation from a third-party organisation selected by the signatories, as foreseen under the Code of Practice;
- An assessment from an independent consultant engaged by the Commission and expected in early 2020;
- A Commission report on the European Parliament elections.

On the basis of this comprehensive assessment, the Commission will decide whether the self-regulatory approach via the Code of Practice on disinformation is satisfactory or whether further regulatory measures should be taken. (TW)

Schengen

Commission: Croatia Ready for Schengen

On 22 October 2019, the Commission issued a Communication in which it confirmed that Croatia meets all necessary conditions for accession to the Schengen area. The Commission also confirmed that Croatia fulfilled commitments undertaken within the framework of the accession negotiations that are also relevant for the Schengen *acquis*. These areas mainly include the good functioning of the judiciary and the respect for fundamental rights.

Croatia declared that it wants to be part of the Schengen regime in March 2015, which triggered a long evaluation and monitoring process whether the country fulfils all parts of the Schengen *acquis*.

Since 2013, this process has been jointly carried out by the Member States and the Commission. They are supported by EU bodies, offices, and agencies; the Commission has an overall coordination role. The Commission prepares and plans the evaluation and adopts evaluation reports, while the Council has the responsibility to adopt recommendations for remedial actions. This is the first time that the new Schengen evaluation and monitoring mechanism has been applied.

A country that wishes to accede must show compliance in a number of policy fields, e.g.:

- In its capacity to take responsibility for controlling the external borders on behalf of the other Schengen States and for issuing uniform Schengen visas;
- In its capacity to efficiently cooperate with law enforcement agencies in other Schengen States, in order to maintain a high level of security once internal border controls are lifted.

The Communication confirmed that Croatia has successfully implemented the Schengen rules in the areas of data protection, police cooperation, common visa policy, return, the Schengen Information System (SIS), firearms, and judicial cooperation in criminal matters. It also affirmed that Croatia meets the Schengen rules on external border management; however, Croatia must work continuously to keep the standard, especially in this field.

It is now up to the Council to verify the evaluation results. The Schengen *acquis* is only applicable after the Council takes a decision giving green light. (TW)

ECA: Use of Information Systems for Border Control Can Be More Efficient

The EU's information systems in the field of internal security supporting border controls are well designed; however, more efforts are needed to ensure completeness and timely entry of the data. This is the main outcome of the European Court of Auditor's special report No 20/2019. The report examined whether the design and use of the major information systems utilised to perform border checks in the Schengen area are efficient. The systems at issue are:

- The Schengen Information System (SIS);
- The Visa Information System (VIS);
- Eurodac (European Asylum Dactyloscopy Database – fingerprint comparison system);
- The European Border Surveillance System (Eurosur);
- The Passenger Name Record systems (PNR).

The auditors found that border guards increasingly use and rely on these systems. The efficiency of border

checks, however, is hampered because some data is currently not included in the systems, while other data is either incomplete or not entered in a timely manner.

Furthermore, it was found that the systems are not used in a uniform way – including a discrepancy between the number of Schengen visas issues and the number of visa checks – which indicates that use of the information in the systems is not systematic.

Regarding the completeness of data, one problem is that officers often receive hundreds of results – mainly false positives – when they check names. This not only impacts efficiency, but also increases the risk of overlooking real hits.

Long delays in putting IT solutions for surveillance and passenger records into practice are another critical point, preventing border authorities from sharing important information efficiently.

The ECA made the following recommendations to the Commission:

- Promote further trainings, especially as regards the use of SIS II and VIS;
- Shorten the time to correct weaknesses identified during Schengen evaluations;
- Analyse discrepancies in visa checks;
- Improve data quality control procedures;
- Reduce delays in data entry.

The Commission provided statements to the ECA's findings and recommendations. The response is annexed to the report. (TW)

Institutions

European Court of Justice (ECJ)

Additional Area Offered on Website

The Court of Justice of the European Union has added a new area to its website, which offers the following information:

- Open access to preliminary ruling cases;
- A compilation of relevant decisions delivered by national courts;
- Notes and studies in relation to research and monitoring works;
- Factsheets on various subjects;
- Legal monitoring documents presenting current legal, judicial, and case-law developments by one or more Member States and by the Courts of the European Union.

The new area is based on the database of the Judicial Network of the European Union (Réseau judiciaire de l'Union européenne, RJUE), which was established in 2017 between the CJEU and participating national courts from the EU Member States. (CR)

New Judges Jääskinen and Wahl

On 7 October 2019, two new judges, *Niilo Jääskinen* and *Nils Wahl*, took up their positions at the Court of Justice.

Niilo Jääskinen, appointed for the period from 7 October 2019 to 6 October 2021, last served as Judge and Vice-President of the Supreme Administrative Court of Finland. He replaces Mr *Allan Rosas*.

Nils Wahl, who last served as Advocate General at the Court of Justice of Sweden, was appointed for the period from 7 October 2019 to 6 October 2024. He replaces Mr *Carl Gustav Fernlund*. (CR)

Presidents of Chambers of the General Court Elected

On 30 September 2019, the Judges of the General Court elected the Presidents of their ten Chambers. The ten presidents elected for the period from 30 September 2019 to 31 August 2022 are *Heikki Kanninen*, *Vesna Tomljenović*, *Anthony Michael Collins*, *Stéphane Gervasoni*, *Dean Spielmann*, *Anna Marcoulli*, *Ricardo da Silva Passos*, *Jesper Svenningsen*, *Maria José Costeira*, and *Alexander Kornezov*. (CR)

New Presidents of the General Court

At the end of September 2019, *Marc van der Woude* was elected President of the General Court for the period from 27 September 2019 to 31 August 2022. Mr Van der Woude has been serving as Judge at the General Court since 2010 and as Vice-President of the General Court since 2016. He succeeds *Marc Jaeger*, who served as President of the General Court from 2007 to 2019.

The newly elected Vice-President of the General Court for the period from 27 September 2019 to 31 August 2022 is *Savvas Papasavvas*. Mr Papasavvas has been serving as Judge at the General Court since May 2004. He succeeds Marc van der Woude. (CR)

New Members of the General Court

For the period from 1 September 2019 to 31 August 2025, the terms of office of the following 12 Judges of the General Court were renewed: Ms *Vesna Tomljenović*, Ms *Mariyana Kancheva*, Ms *Inga Reine*, Ms *Ramona Frendo*, Mr *Anthony Collins*, Mr *Stéphane Gervasoni*, Mr *Eugène Buttigieg*, Mr *Fredrik Schalin*, Mr *Ulf Öberg*, Mr *Jan Passer,* Mr *Alexander Kornezov*, and Mr *Colm Mac Eochaidh*.

In addition, the following persons were newly appointed as Judges of the General Court: Mr *Laurent Truchot* (former Judge at the French Court of Cassation), Ms *Mirela Stancu* (former Director for European Affairs, International Relations and Programmes of the Romanian Superior Council of Magistracy), Ms *Tuula Riitta Pynnä* (former Judge at the Supreme Court of Finland), Ms *Tamara Perišin* (former Special Adviser to the Croatian Ministry of Science and Education), Ms *Petra Škvařilová-Pelzl* (former Legal Secretary at the Court of Justice), Ms *Gabriele Steinfatt* (former Judge at the Higher Administrative Court of Bremen), Mr *Johannes Christoph Laitenberger* (former Director-General of the Directorate-General for Competition of the European Commission), Mr *José Martín y Pérez de Nanclares* (former Director of the Office of the Presidency of the Spanish Council of State), Mr *Rimvydas Norkus* (former President

of the Judicial Council of Lithuania), Mr *Miguel Sampol Pucurull* (former Deputy Director-General of EU and International Affairs at the Abogacía General del Estado (Spanish Ministry of Justice), Mr *Iko Nõmm* (former Judge at the Estonian Court of Appeal), Ms *Ornella Porchia* (former Legal Adviser to the Permanent Representation of Italy to the European Union), Mr *Roberto Mastroianni* (former Adviser to the Italian Government for legislative affairs in the Department of European Affairs), and Mr *Gerhard Hesse* (former Director-General of the Legal Service of the Austrian Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice). The oaths were taken on 26 September 2019, at which time the entry into office of the new Members also took place. (CR)

30th Anniversary of the General Court

On 25 September 2019, the General Court of the European Union celebrated its 30th anniversary. On 25 September 1989, the first members of the Court took up their duties after the General Court of the EU had been set up by a Council Decision of 24 October 1988. (CR)

Building Extension

On 19 September 2019, the Court of Justice of the EU inaugurated its new, fifth extension to the building complex. Among the guests of honour were His Royal Highness, the Grand Duke of Luxembourg; the Prime Minister of the Grand Duchy of Luxembourg, Mr *Xavier Bettel*; the President of the Court, Mr *Koen Lenaerts*; and the architect, Mr *Dominique Perrault*. (CR)

OLAF

OLAF Report 2018

On 3 September 2019, the European Anti-Fraud Office (OLAF) released its annual report for 2018. The key figures for 2018 are:

- OLAF concluded 167 investigations;
- OLAF issued 256 recommendations to the relevant national and EU authorities;
- As a result of the investigations concluded in 2018, OLAF recommended the recovery of €371 million to the EU budget;
- 219 new investigations were opened in 2018.

The report also analyses a number of trends revealed by OLAF's anti-fraud investigations. According to the report, setting up fake companies and disguising falsified business transactions is a very common method used by fraudsters in order to obtain EU funds. Moreover, fraud in the promotion of agricultural products (often in combination with money laundering through third countries) and evasion of customs duties were often investigated by OLAF. OLAF was successful in solving complex, transnational, and intricate cases. This helped not only to stop (organised) criminals from defrauding the EU budget, but also protected the health and well-being of European citizens, as emphasized by OLAF Director-General *Ville Itälä*.

This year's report includes a focus chapter that explains how OLAF cracks down on organized criminals, e.g., fraud in the promotion of agricultural products, organised crime in IT projects, VAT fraud with high-value electronics, etc. The report highlights that OLAF investigators have the necessary experience to quickly identify patterns of fraud and detect new areas of fraud. This is especially the case in cross-border situations in which suspicious behaviour cannot be detected by national authorities alone.

In addition to its investigative work, OLAF also regularly plays a substantial role in the negotiation of legislative instruments on the protection of the EU's financial interests against fraud and corruption. In 2018, OLAF was involved in the development of a new Commission Anti-Fraud Strategy that aims to reinforce OLAF's analytical capacity, the cooperation between OLAF and Commission services, and the Commission's corporate oversight in anti-fraud matters (see eucrim 1/2019, p. 15). As a new task, OLAF will coordinate and monitor the implementation of anti-fraud strategies. OLAF also worked on supporting the entry into force of a new global anti-smuggling treaty, the Protocol to Eliminate Illicit Trade in Tobacco Products, and on a new Commission Action Plan to fight the illicit tobacco trade.

From a legal perspective, a major event in 2018 was the Commission's proposal to amend the Regulation concerning investigations conducted by the European Anti-Fraud Office in order to enable OLAF to complement the work of the new European Public Prosecutor's Office (EPPO) and to ensure a close and effective cooperation (cf. eucrim 1/2018, p. 5 f.). (CG)

Spanish Supreme Court Backs OLAF's Findings on Tuna Customs Fraud

On 6 August 2019, OLAF reported that the Spanish Supreme Court confirmed the findings of OLAF investigations on evaded customs duties with regard to tuna imports from El Salvador. OLAF had investigated allegations of irregularities in tuna exports from El Salvador into the European Union, which did not meet the origin requirements of the EU's Generalised System of Preference scheme.

The investigations extended beyond European borders and involved close cooperation between OLAF, Member States, and third countries. In 2010, OLAF concluded its investigations and recommended the recovery of €9.7 million to the EU budget. Since 2010, the case had been subject to Spanish court proceedings that were concluded in June 2019. The judgment of the Spanish Supreme Court is in line with OLAF's findings and confirms the amount of €9.7 million to be recovered to the EU budget. (CG)

Conference Highlights Need for Strong AFCOS in Candidate Countries

Governments must "give law enforcement and public administration the tools

Report

Workshop on the Network of Associations for European Criminal Law and for the Protection of the Financial Interests of the EU

On 16 September 2019, OLAF organised a one-day workshop to discuss the future of the Network of Associations for European Criminal Law and for the Protection of the Financial Interests of the EU. The workshop took place in Brussels and was attended by 25 practitioners and academics from all over Europe.

The purpose of the workshop was also to encourage the establishment of new associations or for existing associations to join the Network. As a result, the Network was already able to welcome new members, but institutions and associations that might be interested in joining the Network are warmly encouraged to get in contact (info@eucrim.eu).

In her opening speech, OLAF Policy Director *Margarete Hofmann* recalled that the Network, which started with the creation of the first association in Rome in October 1990, will turn 30 next year. Over that period, the protection of the financial interests of the Union had seen an enormous evolution, which culminated in the adoption of the Directive on the fight against fraud to the Union's financial interests by means of criminal law (the PIF Directive) and the Regulation on the establishment of the European Public Prosecutor's Office (EPPO) in 2017. She underlined that the Network has contributed to this success in no small measure, citing the *Corpus Iuris* studies that laid the theoretical foundation for the EPPO. The Honorary President and founder of the Network, *Francesco de Angelis*, provided an overview of the origins and achievements of the Network and made a passionate plea for turning the PIF Directive into a regulation in order to strengthen its uniform application. He also thought that the time is ripe for a more comprehensive codification of European criminal law, both substantive and procedural.

Following this introduction, the workshop was split into four sessions on 'Membership and structure of the Network'; 'Work and priorities' (moderated by Professor *John Vervaele*, Utrecht); 'Annual Meetings and Conferences' (Professor *Rosaria Sicurella*, Catania); and the use of the *eucrim* journal and website (*Thomas Wahl*, MPI Freiburg).

It was agreed to renew efforts to reactivate associations that had become less involved in recent years, as well as to find new members. There was also agreement to identify new topics and strategic projects in which a significant number of network members could get involved, and some suggestions for such topics were made. Finally, it was felt that more importance should be attributed to the annual meetings of the presidents of the associations, by extending their duration and strategic focus. OLAF would organise the annual meeting of the presidents of the associations in 2020 under the new format.

Oliver Landwehr
Legal and Policy Officer, OLAF

they need to detect and to prosecute fraudsters," said OLAF Director-General *Ville Itälä* at the annual conference of Anti-Fraud Coordination Services (AFCOS) in reference to EU candidate and potential candidate countries. The conference was held on 18–20 September 2019 in North Macedonia. It focused on translating operational knowledge into efficient fraud prevention measures.

The conference also highlighted the importance of cooperation between OLAF and AFCOS in the candidate and potential candidate countries in order to protect the EU budget. Between 2014 and 2020, pre-accession funding amounts to €12 billion. AFCOS facilitate the effective cooperation and exchange of information with OLAF. They are active in the implementation of comprehensive anti-fraud strategies at the national level and share information on possible irregularities in relation to the management of EU funds.

OLAF will continue to maintain its investigatory role in candidate countries and potential candidate countries, even after the European Public Prosecutor's Office (EPPO) becomes operational. The EPPO has no jurisdiction to directly investigate fraud in third countries outside the EU. Hence, the solid cooperation established by the OLAF network remains crucial. (TW)

European Public Prosecutor's Office

Ms Kövesi Appointed European Chief Prosecutor

After the decision by the Conference of Presidents (EP President *David Sassoli* and political group leaders) on 17 October 2019, Ms *Laura Codruţa Kövesi* is the first European Chief Prosecutor. She can now start her seven-year mandate. The Council endorsed the nomination on 14 October 2019. The EP and the Council laid their dispute on the candidate to rest in September.

Ms Kövesi, a Romanian national, comes from the Prosecutor's Office attached to the High Court of Cassation and Justice of Romania. She held various positions as prosecutor during her professional career in Romania. She gained renown as chief of the National Anticorruption Directorate (DNA), where she initiated several corruption prosecutions against top Romanian officials.

As European Chief Prosecutor, she will be tasked mainly with organising the work of the EPPO and representing the Office in contacts with EU institutions, Member States, and third countries. She will be assisted by two deputies and will chair the college of prosecutors, which will be in charge of defining strategy and internal rules and ensuring coherence across and within PIF cases. (TW)

State of Play of EPPO Implementation

The Commission informed the justice ministers of the EU Member States on the state of play in implementation of the EPPO Regulation at the JHA Council meeting on 7 October 2019. European Prosecutors who were nominated by the participating Member States were heard by the Selection Panel. However, some Member States still have not submitted their nominations.

The Commission also updated the ministers on other statuses of preparation:

- The EPPO's internal rules of procedure;
- Conditions of employment for European Delegated Prosecutors;
- Creation of the case management system (CMS);
- The EPPO's budget.

As regards the EPPO's inclusion into the Council of Europe conventions (especially the Convention on Mutual Legal Assistance), in order to ensure a smooth cooperation with non-EU countries, the Commission has started informal discussions with the Council of Europe.

The Commission closely accompanies and monitors the necessary adaptations in the legal and administrative framework in the Member States to comply with the EPPO Regulation. To this end, a secured and restricted website was created ("EPPO Wiki"), where Member States have been requested to submit information on the adaptation process.

Lastly, the Commission stressed that full implementation of the PIF Directive is essential, so that the EPPO can start operational business. Some Member States have not notified the Directive's implementation and the Commission started the first phase of the infringement proceedings. (TW)

Europol

Plans for Europol-New Zealand Operational Agreement

Together with its 20th progress report towards an effective and genuine Security Union, the European Commission addressed a recommendation to the Council to authorise the opening of negotiations for an EU-New Zealand agreement. The initiative aims to allow Europol and New Zealand law enforcement authorities to exchange personal data to fight serious crime and terrorism.

The EU and New Zealand agreed on reinforcing law enforcement cooperation in the aftermath of the Christchurch attacks. On the basis of a working agreement signed in April 2019 (see eucrim 2/2019, p. 89), Europol and New Zealand can exchange strategic information, but not personal data.

New Zealand has been taken up on the list of priority countries, which the Commission intends to conclude operational security agreements with in order to combat terrorism, migration, and other forms of serious crime. To date, these countries include those in the Middle East/North Africa (MENA) region. The Commission stressed that the EU and New Zealand are like-minded partners sharing similar views and approaches on many global issues. From Europol's viewpoint, there are common operational interests in the following areas: terrorism, cybercrime (including child sexual exploitation), outlaw motorcycle criminal gangs, and drug trafficking. Europol and New Zealand authorities have successfully worked together in these areas in the past. (TW)

More Cooperation with EUIPO

On 7 November 2019, Europol and the European Union Intellectual Property Office (EUIPO) signed a formal agreement to enhance their cooperation in the fight against intellectual property crime. The agreement continues the work that was already started in 2016, when the two agencies created a specialised unit within Europol that was funded by the EUIPO. Since then, this Intellectual Property Crime Coordinated Coalition (IPC3) has been coordinating and supporting cross-border operations tackling IP crime across the EU. (CR)

Cooperation with Palo Alto Networks

On 23 October 2019, Europol has signed a Memorandum of Understanding (MoU) with Palo Alto Networks, an American multinational cybersecurity company. The MoU enables the exchange of threat intelligence data and details of cybercrime trends as well as technical expertise and best practices, focusing on new adversary behaviours, malware families, and attack campaigns around the world. (CR)

Cooperation with FS-ISAC

On 19 September 2019, Europol's European Cybercrime Centre (EC3) signed a Memorandum of Understanding (MoU) with the Financial Services Information Sharing and Analysis Center (FS-ISAC). Stronger cooperation with the European financial services sector aims to strengthen the law enforcement response to financially motivated cybercriminals targeting banks and other financial institutions. Under the MoU, information sharing will be facilitated, and training exercises and informational summits will be fostered.

FS-ISAC is an industry consortium with almost 7000 member firms and users in over 70 countries. By offering an intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats, FS-ISAC is dedicated to reducing cyber-risk within the global financial system. (CR)

Explanations in 120 Seconds

Europol has launched a new video series explaining law enforcement in 120 seconds. In a series of five clips, the videos illustrate how drugs are produced, trafficked, and distributed by serious and organised criminal organisations, what the negative consequences are for society, and the international law enforcement response to dismantling drug cartels. Drugs make for the largest criminal market in the EU with an EU retail drug market estimated to be worth at least €24 billion a year. (CR)

Europol in Brief 2018

In September 2019, Europol published a brochure offering statistics and updates of Europol's year 2018. In 2018, Europol supported 1748 operations, the majority related to terrorism, cybercrime, and drug trafficking. 8266 operational reports were generated,

mainly in the area of serious and organised crime. With 370 deployments in 2018, Europol's mobile office support was a key feature of its support in 2018: overall, mobile offices were deployed to 43 countries. In addition, a record 1.1 million SIENA (Secure Information Exchange Network Application) messages were exchanged, the top five crime areas being robbery, drugs, fraud, immigration, and terrorism. Another record was achieved with regard to the number of searches conducted in the Europol Information System (EIS), with 4 million searches having been conducted in 2018. This constitutes an increase of 65% compared to 2017. The Europol Platform for experts (EPE) allows its users to share non-personal data on crime and is used by law enforcement in more than 100 countries.

Thanks to the European Union Serious and Organised Crime Threat Assessment (SOCTA), the Internet Organised Crime Threat Assessment (IOCTA), and the EU Terrorism Situation and Trend Report (TE-SAT) (see eucrim news of 9 September 2019), Europol provides a serious of detailed threat assessment reports outlining key threats and trends.

Lastly, citizens are becoming involved in fighting crime via Europol's websites, tracking the EU's most wanted fugitives as well and items leading to locations where child abuse is perpetrated. The 'No more ransom' portal offers decryption for different types of ransomware infections (see eucrim news of 10 September 2019). In 2018, Europol reached its current maximum of staff at 1294 staff members. (CR)

Major Action Day to Tackle EMPACT Priorities

From 5 to 8 September 2019, Joint Action Day (JAD) Western Balkans 2019 was carried out. 6708 officers on the ground, 50 officers in the Operational Centre at Europol's headquarters, and eight agencies and international organisations teamed up to tackle firearms trafficking, illegal immigration, document fraud, and drug trafficking. As a result, 214,147 persons, vehicles, and premises were checked and 175 individuals arrested. (CR)

Eurojust

Cooperation Agreement with Serbia Signed

On 12 November 2019, Eurojust and the Republic of Serbia signed a cooperation agreement allowing for the sharing of personal data and creating the possibility to appoint a Serbian Liaison Prosecutor to Eurojust.

One of the requirements for the cooperation agreement was new Serbian legislation on data protection which meets the EU standards.

Eurojust maintains close connections to the Western Balkan countries: It has already signed cooperation agreements with North Macedonia (2008), Montenegro (2016) and Albania (2018). Before the agreement with Serbia, Eurojust already closely cooperated with the country, e.g., through Serbia's involvement in a number of cases regarding serious organised crime and Serbia's particpation in joint investigation teams that mainly dealt with drug trafficking offences. For Eurojust's collaboration with non-EU countries, see also the article by *Boštjan Škrlec* (in this issue). (CR)

Cooperation Agreement with Denmark

On 7 October 2019, Eurojust and the Kingdom of Denmark signed an agreement to continue their criminal justice cooperation. In light of the new Eurojust Regulation entering into force in December 2019, the agreement was needed to be able to continue judicial cooperation with Denmark, which is a Member State of the European Union but not a Member of Eurojust. Under the agreement, Denmark has the status of an observer at Eurojust College meetings and the possibility to set up a full Desk. It is subject to democratic oversight by its National Parliament and bound by the jurisdiction of the European Court of Justice and the European Data Protection Supervisor. Furthermore, Denmark will financially contribute to Eurojust's budget. In operational terms, Denmark will maintain its access to Eurojust's information systems and be able to second a representative to Eurojust. (CR)

Council Conclusions on Eurojust

At its meeting on 7–8 October 2019, the JHA Council adopted Conclusions on Eurojust, underlining the unique and vital role of Eurojust in the coordination of serious cross-border investigations and prosecution between national investigating and prosecuting authorities.

The Conclusions put emphasis on Eurojust's role and capabilities with regard to digital criminal justice. Key measures in this regard are:

- A strong and modern IT infrastructure and Case Management System (CMS) on the part of Eurojust;
- Access to the e-Evidence Digital Exchange System built by the Commission and operated by Member States.

When looking at other EU agencies, the Council sees Eurojust and Europol as complementary to each other and urges them to continue their efforts to work together closely. Looking at the EPPO, the Council has asked that the EPPO and Eurojust establish and maintain a close relationship and set up a working agreement as soon as possible. Lastly, cooperation between Eurojust and other EU bodies, offices, and agencies, such as OLAF and Frontex, should be continued.

Regarding Eurojust's cooperation with third states, the Council is satisfied with Eurojust's efforts to conclude cooperation agreements with the countries of the Western Balkans. It also encourages the agency to examine the conclusion of cooperation agreements with other third countries.

Looking at the newly created Judicial Counter-Terrorism Register at Eurojust, the Council reminds Member States of their obligation to transmit relevant information to the register.

The entering into force of the new Eurojust regulation as of 12 December 2019 should allow Eurojust to deal more efficiently with the increasing demands of the national authorities, to draft its new rules of procedure, and to implement changes allowing the agency to better concentrate on its operational work. In view of the above, the Council also feels that Eurojust should be provided with adequate financial and human resources. (CR)

New National Member for Lithuania

On 20 August 2019, *Margarita Šniutytė-Daugėlienė* took up her position as National Member for Lithuania at Eurojust. Before joining Eurojust, Ms *Šniutytė-Daugėlienė* served as Deputy Prosecutor General of Lithuania and Chief Public Prosecutor of the 2nd Criminal Prosecution Division at the Regional Prosecutor's Office of Klaipeda. She was also an EJN contact point for several years. Ms *Šniutytė-Daugėlienė* replaces Ms *Laima Čekelienė*, Eurojust National Member for 11 years. (CR)

New National Member for France

On 1 September 2019, *Baudoin Thouvenot* took up his position as National Member for France at Eurojust. Before joining Eurojust, he served as Dean of the Investigative Judges for the Court of Paris and as an investigative judge for the Court of Paris. Mr Thouvenot replaces *Frédéric Baab*, who had served as Eurojust National Member since October 2014. (CR)

Judicial Counter-Terrorism Register Launched

On 5 September 2019, a Counter-Terrorism Register (CTR) was launched (see also eucrim 2/2019). The CTR is managed by Eurojust on a 24-hour basis. In the CTR, key judicial information on proceedings against suspects of all kinds of terrorist offences is centralised, with the aim of establishing links between them and, in this way, helping judicial authorities to more actively coordinate their work and identify the suspects or networks being investigated in specific cases with potential cross-border implications. All Member States can use the CTR and are called upon to register information on suspects and cases via a special template. As the CTR focuses entirely on judicial proceedings and convictions, an overlap with the criminal analysis carried out by Europol is not to be expected. (CR)

Frontex

Cooperation with OSCE

At the beginning of October 2019, Frontex and the OSCE Secretariat agreed on a working agreement to strengthen their co-operation in combating cross-border crime, trafficking in human beings, and in addressing migratory challenges. The agreement covers the following areas:

- Fostering good practices in border management;
- Ensuring fundamental rights protection of people at the borders;
- Developing capacities to address emerging forms of cross-border crime.

The document was signed by OSCE Secretary General *Thomas Greminger* and Frontex Executive Director *Fabrice Leggeri*. (CR)

Operation Mobile 2

At the beginning of October 2019, a 12-day operation, entitled Joint Action Day (JAD) Mobile 2, led to the detection of 439 stolen cars as well to the seizure of 11.9 million cigarettes, 20 tonnes of raw tobacco, 38 firearms and 296 pieces of ammunition, and some 200 kilos of hashish, marijuana, and cocaine. 166 suspected people smugglers, drug smugglers, and persons involved in the possession of smuggled excise goods and weapons were arrested. The operation was led by Frontex and supported by thirteen EU and five non-EU countries, Europol, and Interpol. It also led to the detection of 4365 irregular migrants. (CR)

Seamless Border Control

In October 2019, Frontex – together with the Border Service of Portugal (SEF) and the Lisbon Airport Authority (ANA) – tested new technologies for border control at Lisbon airport to see whether biometric solutions can decrease the waiting time at borders. The technology uses face recognition and touchless scanning of fingerprints with the aim of allowing passengers to pass through border checks without taking out their passports or other documents. The current trial covers EU citizens leaving the Schengen Area. (CR)

Ilkka Laitinen Passed Away

On 29 September 2019, Lieutenant General Ilkka Laitinen passed away at the age of 57. Laitinen was first Executive Director of Frontex upon its establishment, serving from 2005 to 2014. Since 2018, he served as Head of the Finnish Border Guard.

Operation Against Foreign Terrorist Fighters

From July to September, Frontex supported Operation Neptune 2 with two experts to assist in sea border control. The operation was targeted at suspected foreign terrorist fighters potentially using maritime routes between North Africa and Southern Europe. It was coordinated by Interpol and supported by the World Customs Organization (WCO). As a result, more than a dozen suspected foreign terrorist fighters could be detected travelling across the Mediterranean.

Agency for Fundamental Rights (FRA)

Handbook on How to Apply the CFR in Lawmaking and Policymaking at National Level

FRA recently published a handbook offering guidance on use of the EU Charter of Fundamental Rights (the Charter) at the national level. The handbook aims to provide practical orientation on the scope of the Charter based on the

case law of the CJEU. It is targeted at all persons working in national legislative and administrative authorities, such as governments, parliaments, regional and local authorities, and at individuals working in courts and human rights institutions in the EU Member States.

The handbook is structured in three parts – parts I and II and an annex. While the first part offers an introduction to the Charter for all target groups, the second part consists of two checklists designed for persons engaged in legislative and policy processes at the national level. The annex gives a summary of the Charter rights and how they relate to various other human rights catalogues, e.g., the ECHR and human rights' instruments of the UN.

In detail, Part I focuses on the following issues:

- The EU system of fundamental rights protection;
- The Charter's relation to other fundamental rights instruments such as the ECHR;
- Reasons for applying the Charter, its scope of application, and situations in which it applies;
- The interpretation of and limitations on Charter rights.

Part II provides for the following:

- A checklist to assess the applicability of the Charter with regard to national law and policymaking;
- A checklist to promote an initial understanding of whether or not a (draft) national act is in line with the Charter.

The handbook is available in English, Finnish, and French. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

30th Annual PIF Report

spot light

On 11 October 2019, the European Commission published its 2018 report on the protection of the European Union's financial interests – fight against fraud. It is the 30th annual report, the first report having been published in January 1990. Hence, the 2018 report not only contains information about the measures, results, and initiatives in 2018, but also outlines the major achievements of the EU's fight against fraud and the protection of the EU budget over the last three decades. This historical review has also been summarised in the brochure "Protecting the European Union's financial interests – 30 years of joint efforts".

A wealth of information is provided on achievements and challenges in 2018. A first section outlines the cross-cutting policies, measures, and results in 2018 as follows:

- Legislative acts adopted by EU institutions;
- European institutions' legislative and policy initiatives;
- CJEU jurisprudence;
- Measures taken by the Member States;
- Summary of statistics on detected fraud and irregularities.

The report continues with measures and results in the areas of revenue and expenditure. It also covers the following:

- Recovery and other preventive/correctional measures;
- Cooperation with Member States;
- Early Detection and Exclusion System (EDES);
- Follow-up to the European Parliament's resolution on the 2017 PIF report.

The report highlights the following *cross-cutting measures that were adopted*:

- Work on implementation of the Regulation on the establishment of the European Public Prosecutor's Office (EPPO), the Netherlands and Malta having joined to the EPPO in August 2018;
- Regulation (EU, Euratom) 2018/1046, the "Omnibus regulation," which revises the EU's financial rules to simplify them and make them more result-oriented. It includes revisions that simplify the use of financial instruments under the European Structural and Investment Funds. It also redefines conflicts of interest for all financial actors implementing the EU budget in the various management modes, including at the national level;
- Commission proposal to revise Regulation (EU, Euratom) No 883/2013. The revision of the Regulation is primarily driven by the need to adapt the operation of OLAF to the functioning of the future EPPO (see also eucrim 1/2018, pp. 5–6);
- Council Regulation (EU) 2018/1541 on administrative cooperation and the fight against fraud in the field of VAT to increase the capacity of the Member States to address the most damaging VAT fraud schemes and diminish the VAT gap (see eucrim 3/2018, pp. 161–162);
- Commission Anti-Fraud Strategy of 29 April 2019 (see eucrim 1/2019, p. 15 and the article by *Marin/Makri* in this issue).

In addition, the anti-fraud provisions in the legal framework of the next multi-annual spending period 2021–2027 were refined. This includes the persons' obligation to fully cooperate in the protection of the EU's financial interests and to grant access rights to the Commission, OLAF, the EPPO, and the European Court of Auditors (ECA) as well as to other third parties who are involved in implementing EU funded grants.

As regards traditional, own resources (mainly customs duties) on the *revenue side*, detected fraudulent and non-fraudulent irregularities decreased in 2018 compared to the five-year average for the period 2014–2018; however, the financial amount affected was larger.

In 2018, solar panels were the goods most affected by fraud and irregularities in monetary terms as was the case in 2017 and 2016. The most challenging problem, however, remains the undervaluation of goods, in particular footwear and textiles imported from China. Furthermore, fraudsters increasingly abuse the low-value consignment reliefs when it comes to cross-border e-commerce. As a result, the 2018 PIF report makes several recommendations to the Member States; they must enhance and

enforce customs control strategies for cross-border e-commerce trade and ensure the correct collection of traditional, own resources.

As for the *expenditure side*, the report acknowledges that the Member States have put in place a number of measures; however, they differ widely in nature and purpose. In 2018, Member States' operational measures included the introduction of IT risk scoring tools, fraud risk assessments, and training courses to raise general fraud awareness. Statistical data paint a picture similar to that for revenue: fewer fraud cases detected, but a larger financial amount affected.

The report also shows that findings concerning the patterns and conclusions presented in previous annual reports can be verified: as regards the agricultural sector, most problems persist on the local level, which makes prompt action on the part of national authorities necessary. As regards the cohesion funds, improvements were made in 2018, and the strengthened prevention capabilities seem to show promising results. However, the Commission has still to assess whether they are actually due to more efficient systems rather than to under-detection and under-reporting.

As in previous years, the current report calls on Member States to adopt or further develop their national anti-fraud strategies in order to ensure correct spending of EU funds. In this context, the following aspects should be taken into account:

- Risk analysis conclusions contained in the present and previous reports;
- The need to structure the coordination between administrative and criminal checks and investigations;
- Incorporation of tips from the media and from whistleblowers into the control system;
- Opportunity to strengthen the risk analysis-based approach to detect irregularities and fraud, including the use of IT tools.

Since the 2018 PIF report is the last report in the era of the Juncker Commission, it ultimately takes stock of the *achievements during this mandate*. The most important achievements were:

- The Directive on the fight against fraud by means of criminal law (see also eucrim 2/2017, pp. 63–64);
- The Regulation to establish the EPPO by enhanced cooperation (see also eucrim 3/2017, pp. 102–103);
- The revision of the financial regulation (see above);
- The proposal for a targeted revision of OLAF Regulation 883/2013.

When presenting the report *Günther Oettinger*, Commissioner for Budget and Human Resources at the time, also pointed out the launch of the "EU Budget Focused On Results" (BFOR) initiative, which aims at joint efforts on the part of EU institutions, governments, and civil society with a view to better spending, increased accountability, and transparency.

The PIF 2018 report concluded that the new anti-fraud strategy of April 2019 will be the main basis for the new Commission under *Ursula von der Leyen* in order to meet the future challenges posed by the changing environment, in particular by new technologies.

The 2018 PIF report is accompanied by five staff working documents addressing the following issues:

- Implementation of Article 325 by the Member States in 2018 (SWD(2019) 364);
- Statistical evaluation of irregularities reported for own resources, natural resources, cohesion policy and pre-accession assistance, and direct expenditure (SWD(2019) 365 final – part 1, part 2, and part 3):
- Follow-up to recommendations to the Commission report on the protection of the EU's financial interests – fight against fraud, 2017 (SWD(2019) 363 final);
- Early Detection and Exclusion System (EDES) – Panel referred to in Article 108 of the Financial Regulation (SWD(2019) 362 final);
- Annual overview, with information on the results of the Hercule III Programme in 2018 (SWD(2019) 361 final).

The PIF report will now be discussed in the European Parliament, which will issue a resolution on the situation of the protection of the EU's financial interests. (TW)

Council Advances Legislation Against VAT Fraud in E-Commerce

On 8 November 2019, the ECOFIN Council reached a political agreement on future EU legislation that would make VAT-relevant data in e-commerce trade available to anti-fraud authorities. The new rules will oblige payment service providers to keep records of cross-border payments related to e-commerce. These data can then be accessed and analysed by anti-fraud specialists (the "Eurofisc" network). The aim is to facilitate the identification of both EU and non-EU online sellers if they do not comply with VAT obligations. Amendments to the regulation on administrative cooperation in the area of VAT will pave the way for national tax authorities to cooperate in this area in order to detect VAT fraud and control compliance with VAT obligations.

The envisaged legislation has yet to be confirmed by the European Parliament. It is expected that the new rules will apply as of 2024. (TW)

Corruption

Council Discusses Way Forward in Prevention of and Fight Against Corruption

At the JHA Council meeting in Luxembourg on 7 October 2019, the justice ministers of the EU Member States held a debate on EU action against corruption. Points of discussion were:

- Additional action at the EU level to ensure a coordinated, comprehensive and coherent approach to preventing and fighting corruption in EU institutions and Member States;
- Possible added value of an EU-wide

assessment instrument for anti-corruption policies;
- Role of the EU in the global fight against corruption;
- Streamlining and modernization of current EU legislation against corruption.

The ministers mainly agreed that a new, comprehensive EU strategy or action plan to fight and prevent corruption should be developed. In this context, the EU should focus on areas in which the EU's work can bring added value. Possible synergies with existing international instruments should be reviewed in order to avoid duplication of efforts. Lastly, it was concluded that the EU should become a full member of the Council of Europe's Group of States against Corruption (GRECO) in the future, although further discussion is needed as to what this accession would mean for the EU in practice. (TW)

Money Laundering

MEPs Concerned about Member States' Implementation of EU's AML Legislation

On 19 September 2019, MEPs adopted a resolution on the state of implementation of the Union's anti-money laundering legislation. MEPs expressed serious concerns about the lack of implementation of the 4th AML Directive by a large number of Member States and about the fact that the transposition deadlines for the 5th AML Directive in 2020 will also not be met by many Member States.

The resolution also addresses the shortcomings of the EU's fight against money laundering and terrorist financing due to regulatory and supervisory fragmentation, the weak enforcement of EU rules, and inefficient supervision.

MEPs believe that the current legislative approach, by means of which minimum standards are established in the Directives, is a barrier to effective supervision, the seamless exchange of information, and coordination. Therefore, the resolution backs the Commission's plans to replace the Directives by an AML/CFT regulation that would establish a harmonised, directly applicable Union law (see also the AML package tabled by the Commission in July 2019 as reported in eucrim 2/2019, pp. 94–97).

Greater impetus should be given to improving cooperation between the administrative, judicial, and law enforcement authorities within the EU and, in particular, the Member States' Financial Intelligence Units (FIUs).

Ultimately, the resolution favours the establishment of a new methodology to identify high-risk third countries with strategic deficiencies in efficient AML/CTF actions. In this context, the Commission is called on to apply a transparent process with clear and concrete benchmarks for these countries and to ensure public scrutiny. (TW)

ESAs Concerned about ML/TF Monitoring and Reporting

spot light

On 4 October 2019, the European Supervisory Authorities (ESAs) published their second joint opinion on the risks of money laundering (ML) and terrorist financing (TF) affecting the European Union's (EU) financial sector. The opinion is based on Art. 6(5) of Directive (EU) 2015/849, the 4th Anti-Money Laundering Directive (4th AMLD). The provision calls on the ESAs to issue an opinion every two years on the risks of money laundering and terrorist financing affecting the Union's financial sector. The first opinion was issued in February 2017. The "ESAs" are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

The ESAs' report is based on information provided by national anti-money laundering (AML) and countering the financing of terrorism (CFT) competent authorities (CAs) and on information obtained in the context of the ESAs' work.

Underpinning the risk-based approach introduced by the 4th AMLD, the joint opinion is, above all, designed to help identify, understand, manage, and mitigate the risks of money laundering and terrorist financing that the EU and its Member States face. The risks are grouped into two broad categories: cross-sectoral risks and sector-specific risks. The opinion identifies the following issues as the main ML/TF risks that cut across all sectors:
- The UK's withdrawal from the EU which, inter alia, results in relocations of companies, thus making adequate supervision difficult;
- New technologies, making it difficult to understand new products and services available to credit institutions;
- Virtual currencies, bringing about challenges due to the absence of a common regulatory regime and the anonymity associated with them, and requiring CAs to engage in more cooperation with the private sector;
- Divergent national legal frameworks: although this is a direct consequence of the minimum level of EU harmonization, diverging transposition especially in the area of prevention of the use of the financial system for the purpose of ML/TF is apparent;
- Divergent supervisory practice: here, the CAs' engagement in the same sector varies significantly; in some sectors, a large number of CAs do not even carry out an assessment of controls;
- Weaknesses in the implementation of internal controls within firms, in particular as regards customer due diligence;
- Application of non-adequate de-risking methods, i.e., a firm's decision to no longer offer services to some categories of customers associated with a higher ML/TF risk, which leads to the increased use of informal and unregulated channels by customers.

The ESAs propose a number of actions to the CAs, which could mitigate the identified ML/TF risks. These include:
- Better cooperation and information exchange between CAs and UK authorities in order to cope with the chal-

lenges that result from re-establishment of firms in EU Member States following the UK's withdrawal from the EU;
- Familiarization with new technical developments, in particular in the FinTech and RegTech sectors, and engaging directly with private companies;
- Close monitoring of developments associated with virtual currencies and assessment of whether changes to the AML/CFT regulatory and legal framework is required;
- Setting of clear regulatory expectations as regards internal controls, taking account, for instance, of the ESAs' risk factor guidelines;
- Support for the exchange of information and cooperation between law enforcement, firms, and CAs;
- Guidance for the de-risking policies of the firms.

In the second section, the opinion examines the risks in specific sectors, e.g., credit institutions, life insurance companies, payment institutions, bureaux de change, investment firms, etc. Each sector is assessed according to the following five aspects:
(1) Inherent risk in the sector;
(2) Quality of controls and common breaches in the sector;
(3) Overall risk profile of the sector;
(4) Emerging risks in the sector;
(5) Recommendations for the CAs.

In the sector-specific context, the ESAs are alarmed by the fact that a number of CAs have not carried out an assessment of controls in certain sectors. Poor quality controls result in a higher number of breaches.

An interactive tool, available on the EBA website, completes the joint opinion. It provides a snapshot of all ML/TF risks covered in the joint opinion. (TW)

Tax Evasion

Commission: Benefits of Administrative Cooperation in Direct Taxation Unclear

On 12 September 2019, the Commission presented its first evaluation report on Directive 2011/16/EU regarding administrative cooperation in the field of taxation. The Directive lays down rules and procedures for the cross-border exchange of tax information between the national tax administrations. The Directive has been applied since January 2013. It aims at effectively managing the taxpayer's obligations and preventing tax evasion in his/her country of residence rooted in abuse of the freedom to move, operate, and invest across national borders. In the end, the Directive shall contribute to fairer taxation and transparency.

The information in the evaluation report is based on a study by an external contractor, on material provided by the tax administrations of the EU Member States, and on earlier Commission reports in the area of administrative tax cooperation. The report aims to analyse the application of the Directive according to five fundamental aspects: effectiveness, efficiency, coherence, relevance, and EU added value.

The evaluation report mainly concludes that assessment of the aspects was difficult because the evidence submitted was limited and thin. For most Member States, there is no answer to the question of whether the needs addressed by the Directive have been met in an efficient and effective way. In particular, the monetary benefits of the Directive's mechanisms remain unclear. For the next evaluation cycle, the Commission will focus more strongly on obtaining clearer information from Member States on the use of the information exchanged. (TW)

EP: Plans to Set up a Subcommittee on Tax and Financial Crime

In September 2019, the coordinators of the Economic and Monetary Affairs Committee (ECON) in the European Parliament officially decided to create a permanent subcommittee on tax and financial crime. The initiative was mainly propelled by the Greens/EFL Group, which feels that the new subcommittee is needed to follow up on special or inquiry committees that were established in the aftermath of several tax avoidance scandals, such as the Panama Papers or LuxLeaks. The subcommittee would be the successor to the special committee TAX 3, which had continued the work of the ad hoc committees TAXE, TAX2, and PANA. In its final report of 26 March 2019 on financial crimes, tax evasion, and tax avoidance, TAX 3 stated that "there is an urgent and continuous need for reform of the rules, so that international, EU and national tax systems are fit for the new economic, social and technological challenges of the 21st century."

The permanent subcommittee can build on the work of the previous committee and investigate tax evasion, tax avoidance, and money laundering. It could become a major driving force for reform legislation, preventing multinational companies from failing to pay corporate taxes or a small amount of taxes on their profits in Europe.

"The decision is a victory for all of us who want to see an end to the dodgy tax practices and illicit activities that undermine the global financial system and fracture our societies," *Sven Giegold* said. *Giegold* is a German MEP from the Green Party and one of the initiators of the decision.

The establishment of the subcommittee has yet to be approved by the Conference of Presidents of the Parliament, and the precise mandate has yet to be agreed. (TW)

Cybercrime

The Current Cybercrime Landscape: IOCTA 2019

spot light

On 9 October 2019, Europol published its 2019 Internet Organised Crime Threat Assessment (IOCTA). The 2019 IOCTA provides key findings and recommendations regarding the cybercrime threat landscape, focusing on six crime priorities:

- Cyber-dependent crime;
- Online child sexual exploitation;
- Payment fraud;
- Criminal abuse through the Darknet;
- The convergence of cybercrime and terrorism;
- Cross-cutting crime factors.

Looking at cyber-dependent crime (meaning any crime that can only be committed using computers, computer networks, or other forms of information communication technology), the overall volume of ransomware attacks has declined. Attackers seem to focus on fewer but more profitable targets. Nevertheless, ransomware remains the most significant threat in the field of cybercrime. In its recommendation on how to tackle cyber-dependent crime, the report finds that targeting major crime-as-a-service-providers is the most successful approach. Furthermore, the report recommends the following:

- Strong cooperation between law enforcement and the private sector;
- Collaboration between the network and information security sector and cyber law enforcement authorities;
- The use of existing cooperation channels.

Low-level cybercrimes should also be targeted as a means of intervention in the criminal careers of young, developing cybercriminals.

As regards child sexual exploitation online, the report finds a continued increase in available child sexual exploitation material (CSEM), self-generated explicit material (SGEM), and even live distant child abuse (LDCA). In order to reduce CSEM material, the report recommends coordinated action with the private sector and the deployment of new technology, a structural educational campaign across Europe, and law enforcement cooperation with developing countries. One concrete measure to prevent child sex offenders from travelling to third countries to sexually abuse children would be the use of passenger name record (PNR) data by EU law enforcement authorities (accessible through the Travel Intelligence team within Europol).

In the area of payment fraud, the report sees CNP (card not present) fraud as the main priority; however, skimming also continues to evolve as do jackpotting attacks. To combat payment fraud, the report recommends cooperation between the public and private sectors, the exchange of information, training of employees, and raising awareness among customers.

The report emphasizes the key role of the Darknet in the increasing number of single-vendor shops and smaller, fragmented markets as an enabler of trade in an extensive range of criminal products and services. To combat criminal abuse through the Darknet, the report identifies the following measures as key:

- Coordinated investigation and prevention actions;
- The ability to maintain accurate real-time information;
- Improved coordination and standardisation of undercover online investigations;
- An EU-wide legal framework to clarify jurisdiction despite anonymity issues.

Challenges with regard to the convergence of cybercrime and terrorism include the wide array of online service providers (OSPs) and the use of new technologies being exploited by terrorist groups. To counter terrorist groups' online propaganda and recruitment operations, the report recommends addressing the entire spectrum of abused OSPs. In order to manage a crisis after a terrorist attack, the report emphasizes the need for cross-platform collaboration and a multi-stakeholder crisis response protocol on terrorist content online.

New cross-cutting crime factors include hackers and fraudsters now routinely targeting crypto-assets and enterprises. In order to tackle these factors, the report recommends that law enforcement develop and share knowledge with the judiciary, establish relationships with cryptocurrency-related businesses, and share information with Europol. (CR)

Guidelines and Recommendations on Spear Phishing

On 4 November 2019, Europol's European Cybercrime Centre (EC3) published a report on how to prevent, respond to, and investigate spear phishing attacks.

Spear phishing describes the practice of targeting specific individuals within an organisation or business for the purposes of distributing malware or extracting sensitive information.

The report gives an overview of the threat of spear phishing from the perspective of law enforcement and industry. It explains the background of the concept of spear phishing, outlines the most common *modi operandi*, and offers guidance and recommendations on technical solutions, prevention, and awareness as well as on attribution and operational response.

According to the report, email is the most widely used vector for spear phishing. The most commonly used modus operandi is reconnaissance, i.e., deceiving the target. In order to achieve this aim, phishing emails try to include as much content that is familiar to the recipient as possible. Information used to create this familiar content is usually simply found online.

When attacking, a fraudulent link is often sent, leading to a replica of a trusted website (phishing site). Attackers also attempt to make the target download and open a malicious file in order to gain access to the system. Business Email Compromise (BEC) is often aimed at convincing employees to transfer large sums of money to the criminal's bank account.

Depending on the goal of the attacker, the target's files may be encrypted and a ransom payment (ransomware) demanded, remote control may take over the target's system (Remote Access Trojan), relevant credentials may be stolen (key loggers), or the network may be monitored and files extracted.

In order to respond to phishing, the report recommends two sorts of technical solutions, namely policies and software. By means of security policies, users can be prevented from engaging in risky behaviour. Commercial and open source software solutions can help mitigate the threat of phishing and automatically detect phishing attempts. Furthermore, the report recommends investing in prevention and awareness raising measures to establish a resilient user base, e.g., by offering anti-phishing training to employees.

When launching an investigation, law enforcement should have in place procedures and methods for handling this type of incident, e.g., reporting tools between the private sector and law enforcement and other public-private partnerships.

In order to reduce abuse of the Domain Name System (DNS), the report recommends that registrars and registries adopt aggressive anti-abuse measures. Ultimately, the report regrets the loss of the WHOIS data. The WHOIS database contained personal information on registrants of domain names. Law enforcement have no longer direct access due to the new GDPR rules. (CR)

Cyber-Attack Simulation Exercise

On 31 October 2019, Europol conducted the first law enforcement exercise of this kind (CyLEEx19), simulating a cross-border cyberattack on critical infrastructure. The exercise, which was organised by EC3 and ENISA, brought together 20 cybercrime investigators and cybersecurity experts from the public and private sectors. By means of a faked scenario, participants were asked to test the EU Law Enforcement Emergency Response Protocol (see eucrim news of 13 May 2019) by reacting to, responding to, and collectively deciding on simulated large-scale cyberattacks. The attacks were related to incidents, such as misuse of IT resources, unauthorised access to systems, vulnerability exploitations, Distributed Denial of Service (DDoS), and malware infections. (CR)

Racism and Xenophobia

Regulation on Removal of Internet Content Promoting Terrorism – State of Play

On 24 September 2019, the European Parliament's LIBE Committee backed the position, as agreed by the plenary before May's European elections, on the proposed Regulation seeking prevention of the dissemination of online content promoting terrorism (for the EP's resolution of 17 April 2019, see eucrim 1/2019, p. 21). The LIBE Committee's decision paved the way for the start of negotiations with the Council on the legislative dossier. The Council already agreed on its position in December 2018.

MEPs accented that the following points are important in their position:

- Obligation for internet companies to remove content promoting terrorism within one hour of receiving an order from national authorities;
- Regarding sanctions, companies that systematically and persistently fail to abide by the law should be fined up to 4% of their global turnover;
- Implementation of a clause that protects free speech and press freedom;
- Obligation for hosting service providers to establish user-friendly complaint mechanisms;
- No obligation for hosting service providers, such as Facebook or YouTube, to proactively identify terrorist content, because this would be a too great a burden for these platforms; monitoring the information or actively seeking facts indicating illegal activity should be the responsibility of the competent national authority only;
- No obligation to use filters or automated tools;
- Increased support for small platforms, which may not be familiar with removal orders.

Swift agreement on the new EU rules to tackle the dissemination of terrorist content online is one of the priorities of the EU's security policy. (TW)

Procedural Criminal Law

Procedural Safeguards

Commission Implementation Report on Access to Lawyer Directive

On 27 September 2019, the European Commission published its implementation report on Directive 2013/48/EU on the right of access to a lawyer. The Directive is one of the six EU procedural rights directives that aim to harmonise safeguards of suspected or accused persons in criminal proceedings throughout the European Union.

The so-called A2L Directive ensures, *inter alia*, that individuals have a lawyer from the first stage of police questioning and throughout criminal proceedings. Adequate, confidential meetings with the lawyer are also guaranteed. In European Arrest Warrant proceedings, the Directive lays down the right of access to a lawyer in the executing EU country and the right to appoint a lawyer in the issuing country.

Beyond the right of access to a lawyer, the Directive also includes the rights for persons deprived of their liberty to have a third person informed thereof, to communicate with third persons, and to communicate with consular authorities/ to have legal representation arranged for by them.

The report concludes that considerable progress has been made in the protection of fair trial rights in the EU, but difficulties regarding key provisions of the Directive exist in a number of Member States.

Points of concern are as follows:

- The scope of rights enshrined in the Directive: some jurisdictions require a formal act that triggers the right of access to a lawyer or do not apply the right to persons who have not been deprived of liberty;
- The extent of possible derogations;
- Waiver of the right of access to a lawyer;
- Conditions governing how people

can access a lawyer in the issuing Member State of a European Arrest Warrant.

On 12 November 2019, the Commission discussed the report with MEPs in the EP's LIBE Committee. The Commission announced that it will continue to assess Member States' compliance with the Directive and take every appropriate measure, including possible infringement proceedings, to ensure conformity with the provisions of the Directive throughout the European Union.

The Commission's implementation report comes alongside a report from the Fundamental Rights Agency on the practice of eight EU Member States. The latter investigated the implementation of certain defence rights, including the right to be advised and represented by a lawyer. (TW)

FRA Report on Information about Defence Rights and Rights to Access to a Lawyer

spot light

Full access to justice is not guaranteed, at least not in an equal way, because defendants are often poorly informed or access to legal assistance is inadequate. This is one of the main results of a report issued by the European Union Agency for Fundamental Rights (FRA) on 27 September 2019.

The report entitled "Rights in practice: access to a lawyer and procedural rights in criminal and European arrest warrant proceedings" summarises the views of over 250 interviewed professionals and defendants in eight Member States: Austria, Bulgaria, Denmark, France, Greece, the Netherlands, Poland, and Romania. FRA investigated how the following defence rights of suspected or accused persons (set out in primary and secondary Union law) are implemented in said Member States in practice:

- Information about defence rights;
- Right to be advised and represented by a lawyer;
- Rights of persons arrested on the basis of an EAW.

Key findings of the report include:

- Information provided to defendants differs in both scope and content and in how it is conveyed;
- Treatment of defendants other than a suspect at the initial stage of the criminal proceedings, lack of practice on the part of police officers, lack of practice in verifying defendants' understanding of the situation or identifying his/her vulnerabilities, and other factors lead to defendants not being fully aware of their procedural rights;
- Defendants very often receive minimal or unclear information about the charges against them;
- Sometimes individuals are questioned as witnesses or are "informally" asked questions instead of being treated suspected persons; in this way, persons are deprived of their right to remain silent and not to incriminate themselves;
- Police officers sometimes discourage defendants from exercising their right to a lawyer;
- Particularly people who are deprived of their liberty often do not receive legal assistance promptly and directly;
- Defendants deprived of liberty are not always allowed to talk to their lawyers in private before their first questioning; instead, conversations with lawyers are short or take place in public corridors in the presence of police officers;

As regards the specific case of upholding defence rights in EAW proceedings, the report mainly discovered the following:

- Many respondents said that they did not understand their rights as regards warrants and the meaning of their consent to surrender;
- Language barriers often impede the effective enjoyment of rights in EAW cases;
- Defendants regularly face significant difficulties in establishing a double defence, i.e., not only access to a lawyer in the executing, but also in the issuing State. The reasons for this are manifold, including linguistic difficulties, police officers' lack of knowledge, and unwillingness to interfere in another country's jurisdiction. The report revealed systemic deficiencies in the context of the executing authorities' obligations to inform on and assist in appointing a lawyer in the issuing state.

The FRA report includes several recommendations to the Member States on how to improve the effective exercise of said defence rights and to remedy the detected flaws. The FRA report is a preparatory work which the Commission asked for. It complements the Commission report on how EU Member States have implemented the EU's Access to a Lawyer Directive. This report was issued on the same day as the FRA report. Furthermore, the FRA reported on earlier FRA activity on procedural rights, such as the 2016 report on Member States' legal frameworks, policies, and practices regarding the right to information, translation, and interpretation in criminal proceedings (see eucrim 4/2016, p. 163). (TW)

CJEU: Scope of EU's Procedural Rights Directives in Procedures Ordering Committal to Psychiatric Hospital

On 19 September 2019, the CJEU delivered a judgment dealing with the applicability and interpretation of the procedural rights directives in a situation where the judicial authorities of a Member State ordered a person be committed to a psychiatric hospital. The case (C-467/18 – *criminal proceedings against "EP"*) was brought to the CJEU by a Bulgarian court, which voiced doubts as to whether the Bulgarian provisions governing compulsory admission of mentally ill persons to a medical facility are in conformity with the rights guaranteed in Directive 2012/13 (right to information), Directive 2013/38 (access to a lawyer), Directive 2016/343 (presumption of innocence), and the Charter of Fundamental Rights of the EU.

The referring court has to deal with the legality of the procedure against "*EP*" who killed his mother in a state of paranoid schizophrenia and was ordered to adopt compulsory medical measures by means of a special proce-

dure defined in the Bulgarian code of criminal procedure.

First, the CJEU dealt with the question of the applicability of Directive 2012/13 and Directive 2013/48. By above all referring to the wording of the provisions on the applicability of the Directives (Articles 2 of each) and on the interpretation of the fundamental right to liberty and security (as enshrined in Art. 6 CFR, Art. 5 ECHR), the CJEU concluded that the Directives' scope covers judicial proceedings in which an order may be made for the committal to a psychiatric hospital of a person who, at the conclusion of earlier criminal proceedings, was found to be the perpetrator of acts constituting a criminal offence. As a consequence, this person must also be informed of his/her rights as soon as possible, at the latest before his/her first official questioning by the police.

Second, the CJEU ruled on the review powers of the national court. In this context, the CJEU considers national legislation not to be in line with EU law (right to an effective remedy) if the court is not able to rule on the respect of procedural safeguards in the proceedings that took place prior to those before the court.

Third, the CJEU clarified, however, that Directive 2016/343 on the presumption of innocence does not apply if the order for the committal to a psychiatric hospital was based on a law aiming at preventing danger, such as the Bulgarian Health Law. As a consequence, EU law is not the yardstick to assess whether the rights enshrined in the Directives were upheld in such preventive procedures.

However, Art. 3 of Directive 2016/343 is applicable if the judicial proceedings for the committal to a psychiatric hospital and thus the deprivation of liberty do not pursue merely therapeutic, but also safety purposes. Therefore, the public prosecutor's office has the burden of proof that the person whose admission is sought is the perpetrator of acts deemed to constitute such a danger. (TW)

Data Protection

Security Union: Commission Wants Mandate for EU-Japan PNR Agreement

During the EU-Asia Connectivity Forum held in Brussels on 27 September 2019, Commission President *Jean-Claude Juncker* announced that the Commission recommended that the Council give green light to open negotiations with Japan on the transfer of Passenger Name Records (PNR). PNR are travel information data necessary to enable reservations to be processed by air carriers. Nowadays, PNR data are considered a building block in preventing and prosecuting terrorism and serious crime.

The Commission's recommendation to the Council to authorise the opening of negotiations for an EU-Japan PNR agreement (COM(2019) 420 final) is accompanied by an annex setting out directives for the negotiations. The directives define not only the objectives of the envisaged agreement but also the parameters necessary to safeguard and control respect for the protection of personal data, fundamental rights, and freedom of individuals, irrespective of nationality and place of residence, in the context of the transfer of PNR data to Japan.

The Commission's initiative concretely implements an idea in the EU-Japan Strategic Partnership Agreement (signed in July 2018), which specifically encourages both parties to use "available tools, such as passenger name records to prevent and combat acts of terrorism and serious crimes." The agreement aims at further strengthening the key strategic partnership between the EU and Japan in the fight against terrorism and other forms of serious crime. The EU already concluded an agreement on mutual legal assistance in criminal matters with Japan for this purpose.

Currently, the EU has two PNR schemes in force with Australia and the United States of America. The EU is also negotiating a PNR agreement with Canada after the CJEU declared a previously planned agreement with Canada void in 2017 (see eucrim 3/2017, pp. 114–115). The transfer of the PNR data of passengers on international flights to the European Union (EU) countries and the processing of these data by law enforcement authorities in the EU Member States is regulated by the EU PNR Directive 2016/681 (see also eucrim 2/2016, p. 78). At the global level, the International Civil Aviation Organisation (ICAO) is currently working with its Member States to establish a standard for the processing of PNR data.

Regarding the envisaged EU-Japan PNR accord, it is now up to the Council to consider the recommendation and to adopt a Decision authorising the Commission to open negotiations. (TW)

EU Governments Look into Future of Interoperability

After having agreed on the legal framework of the interoperability of EU Information Systems designed for border/migration control and police/judicial cooperation (see eucrim 2/2019, p. 103), delegations from the Member States' governments are now discussing further extensions. The Finnish Council Presidency continued discussions that started earlier this year during the Romanian Presidency to explore further needs of law enforcement and possible EU support (see the discussion paper of 6 September 2019, published by Statewatch).

The Council Presidencies aim at driving forward interoperability through automation. Discussions have, for instance, taken place on possibilities to interconnect queries through the Prüm regime (featuring cross-border access to DNA, dactyloscopic and vehicle registration databases) with the centralised EU information systems. The Council Presidency also referred in this context "to increased interoperability, which means adding possibilities for end users to reach new data sources with a single query." The latter also means including new data categories into the Prüm regime, e.g., firearms, driving licences, or facial images. Another aspect concerns

making data held at Europol interoperable with other EU-level data, where projects are already running.

The discussion paper also mentions other ongoing projects that promote automation and interoperability, such as EPRIS-ADEP – a system for making available certain biographical data contained in national police records.

It concludes that the EU should not stop at the implementation of the agreed interoperability package of May 2019 and a potential reform of the Prüm regime, but take a proactive approach to the future of interoperability. (TW)

Federal Administrative Court Refers German Data Retention Law to European Court of Justice

On 25 September 2019, the German Federal Administrative Court (*Bundesverwaltungsgericht*) decided to refer to the European Court of Justice in order to clarify whether the German data retention law is compatible with Union law.

The German Federal Administrative Court now has to decide on the lawsuits of an Internet provider and a telephone provider who are opposing their obligation to retain the telecommunication traffic data of their users as laid down in Sections 113a, 113b of the Telecommunications Act. According to these provisions, introduced in the new German data retention law of 2015 (the first national law implementing the Data Retention Directive 2006/24/EC having been declared unconstitutional by the German Federal Constitutional Court – FCC), telecommunications providers are obliged to retain the traffic data of their users for a period of 10 weeks and location data for four weeks in order to be able to provide them to the law enforcement authorities, if necessary. The retained data may only be used by the authorities for the prosecution of serious criminal offences or for the prevention of danger to the life, body, or freedom of a person or of threats to the existence of the Federation or a Land (§ 113c Telecommunications Act).

In the previous instance, the Administrative Court (*Verwaltungsgericht*) of Cologne had stated that the applicants were not obliged to retain the telecommunication traffic data, arguing that this obligation set by the German data retention law contravenes European Union law. As a result of a previous, very similar decision by the Higher Administrative Court of Münster (cf. eucrim 2/2017, p. 71), the Federal Network Agency (*Bundesnetzagentur*) has already decided not to enforce the retention obligations for telecommunications and Internet providers for the time being.

The Administrative Court of Cologne and the Higher Regional Court of Münster both referred to the judgment of the CJEU of 21 December 2016, in cases C-203/15 and C-698/15, *Tele 2 Sverige et al.* (cf. eucrim 4/2016, p. 164), which established very narrow conditions for national laws to maintain data retention rules. This decision has led to serious doubts on whether there is a general prohibition of blanket retention systems that can be justified neither by the gravity of threats to public security nor by stringent security and access requirements.

The CJEU found in its judgment that the British and Swedish legislations on data retention were not compatible with Union law. Compared to the British and Swedish legislation, however, the German provisions are more restrictive (e.g., in terms of the period of retention) and set strict security and access rules in order to protect the data. The German Federal Administrative Court therefore decided not to simply take over the findings of the 2016 judgment, but to make reference for a preliminary ruling to the CJEU.

The judges in Luxembourg now have to deal with the question of whether a national law (and the German data retention law in particular), providing a blanket retention measure that clearly interferes with Art. 5 of Directive 2002/58/EC, can be justified under Art. 15 of the same directive or whether it is generally forbidden by Union law. If the Court finds that the German data retention law contravenes Union law, it will not be applicable anymore due to the primacy of Union law.

There is also a complaint against the current German data retention law pending before the FCC. The Constitutional Court has repeatedly dismissed motions for a temporary injunction, arguing that, even after the CJEU 2016 decision, questions still remain that are not suitable for clarification within summary proceedings. It is uncertain whether a final Constitutional Court decision can be expected soon.

In addition to the reference from Germany, courts in Belgium, France, and Estonia referred questions to the CJEU regarding the compatibility of their countries' data retention legislation with EU law, notably Art. 15 of Directive 2002/58/EC ("the e-privacy Directive") – see pending cases C-520/18; C-511/18; and C-746/18 (see also eucrim 1/2019, p. 26). The Investigatory Powers Tribunal, London, posed the question on applicability of the "*Tele2 Sverige/Watson* requirements" in the national security field (Case C-623/17). (CG)

Victim Protection

CJEU: Victims of Crime Can Be Re-Examined if Judge's Bench Changed

By judgment of 29 July 2019, the CJEU shared the opinion of Advocate General *Yves Bot* in case C-38/18 (*criminal proceedings against Massimo Gambino and Shpetim Hyka*), namely that Arts. 16 and 18 of Directive 2012/29/EU establishing minimum standards on the rights, support, and protection of victims of crime do not preclude national rules. According to the national rules, re-examination of a victim is held necessary if the judge's bench changes and the defence counsel of the accused persons do not consent to the court reading the written record of the oral evidence previously

given by that victim. For the opinion of AG *Bot* and the underlying Italian rules that triggered the reference for a preliminary ruling, see eucrim 1/2019, pp. 28–29.

The CJEU stresses that the victim's right to be protected from secondary and repeated victimization is without prejudice to the accused persons' defence rights and their right to a fair trial. It also refers to the case law of the ECtHR highlighting the importance of questioning witnesses before the deciding judge.

However, the ECtHR case law also indicates that the Member States must recognise particular circumstances that may justify a waiver of witness examination if it is not important for the conviction. Hence, re-examination of the victim is permitted if the court in the main proceedings does not identify specific protection needs that would make specific protection measures necessary pursuant to Arts. 23 and 24 of Directive 2012/29. This is up to the referring Italian court to decide. (TW)

Cooperation

Judicial Cooperation

Entry into Force of Surrender Agreement Between European Union and Norway/Iceland

On 28 June 2006, the European Union, the Republic of Iceland, and the Kingdom of Norway entered into an agreement on the surrender procedure between the Member States of the European Union and Iceland and Norway. The agreement aims at improving the surrender procedure for the purpose of prosecution or execution of a sentence between the EU Member States and Iceland and Norway. The expedited extradition procedures are largely based on the European Arrest Warrant model (cf. eucrim 1–2/2006, p. 19).

According to the final provisions, the agreement enters into force on the first day of the third month following the day on which the Secretary-General of the Council of the European Union has found that all formal requirements (especially the deposit of the notifications and declarations) have been fulfilled. With the submission by Italy of its notifications and declarations on 29 August 2019, all EU Member States, Iceland, and Norway have now deposited their declarations and notifications. Accordingly, the formal requirements have been fulfilled and the Agreement entered into force on 1 November 2019. The library of the European Judicial Network provides further information about the notifications and declarations and other useful details. (CG)

Eurojust Guidelines: Deciding on Competing Requests for Surrender and Extradition

Eurojust published a revised version of its guidelines for deciding on competing European Arrest Warrants (EAWs) of 2004. The new guidelines enlarge the scope of the original guidelines, including scenarios for both the situation of multiple EAWs and the situation of conflicts between an EAW and a request for extradition presented by a third country (Art.s 16 (1) and (3) of Council Framework Decision 2002/584/JHA).

By means of five scenarios, the revised guidelines give advice on how to proceed in the situations when two or more EAWs against the same person were issued:
(1) for prosecution of the same offence(s);
(2) for prosecution of different offences. Furthermore:
(3) when two or more EAWs against the same person, of which one (or more) EAW(s) for prosecution and one (or more) EAW(s) for the execution of a custodial sentence or a detention order in relation to different offences, were issued;
(4) when two or more EAWs against the same person for the execution of two (or more) custodial sentences or detention orders in relation to different offences were issued;
(5) when one or more EAW(s) and one (or more) request(s) for extradition were issued. (CR)

European Arrest Warrant

CJEU: Executing Judicial Authority Must Make Precise Assessment of Detention Conditions

spot light

On 15 October 2019, the CJEU (Grand Chamber) further clarified its case law as to the conditions under which the surrender of a person sought by a EAW can be refused because standards of detention in the issuing state infringe the prohibition of inhuman or degrading treatment (Art. 4 of the Charter of Fundamental Rights). The judgment follows the landmark judgment *Arranyosi and Căldăraru* (case C-404/15, see eucrim 1/2016, p. 16), and the judgment in case C-220/18 PPU (*Generalstaatsanwaltschaft [conditions of detention in Hungary]*, also referred to as "Aranyosi III", see eucrim 2/2018, pp. 103–104).

➤ *Background of the Case:*

The judgment of 15 October 2019 was triggered by a request for a preliminary ruling from the Higher Regional Court (*Oberlandesgericht*) of Hamburg, Germany regarding the execution of a EAW against Mr Dorobantu for the purpose of conducting criminal proceedings in Romania (case C-128/18). After having initially approved his surrender, the execution was halted by the German Federal Constitutional Court. The FCC argued that the Higher Regional Court of Hamburg had to file a preliminary ruling to Luxembourg because the legal questions at issue had not been precisely decided in the Kirchberg's courtrooms. For the case history, see eucrim 1/2018, pp. 32–33.

The Hamburg Court mainly put forward four queries:

- Extent and scope of the review by the executing judicial authority if it possess-

es information showing that there are systemic and generalized deficiencies in detention conditions in the issuing state;
- Standards for the assessment of space per detainee in a prison cell;
- Influence of existing legislative and structural measures that improve detention conditions in the issuing state on the assessment;
- Possibility to weigh a fundamental rights infringement against the efficacy of judicial cooperation in criminal matters and the principles of mutual trust/recognition.

➤ *The CJEU's Judgment – Parameters:*

The judges in Luxembourg essentially follow the opinion of Advocate General *Manuel Campos Sánchez-Bordona* presented in April 2019 (see eucrim 1/2019, p. 36).

If an executing judicial authority assesses a real risk of inhuman or degrading treatment within the meaning of Art. 4 of the Charter, it must take into account all the relevant physical aspects of the conditions of detention in the prison in which the person subject to surrender will be detained, e.g., the personal space available to each detainee in a cell in that prison, sanitary conditions, and the extent of the detainee's freedom of movement within the prison. One precondition remains, however, namely that the executing authority affirms systemic and generalised deficiencies in the detention conditions of an issuing Member States.

Regarding the personal space available to each detainee, the executing judicial authority must take account the minimum requirements set by the ECtHR when interpreting Art. 3 ECHR. The CJEU stresses that the detainee must (at least) have the possibility to move around normally within the cell. The Court also refers to its previous case law in which it indicated that "a strong presumption of a violation of Article 3 of the ECHR arises when the personal space available to a detainee is below 3 m^2 in multi-occupancy accommodation."

Possible legal remedies and control mechanisms in the issuing state cannot rule out the existence of a real risk of inhuman or degrading treatment. In addition, the executing judicial authority cannot weigh up a found risk of the fundamental right's infringement against considerations relating to the efficacy of judicial cooperation in criminal matters and to the principles of mutual trust and recognition.

➤ *Put in focus:*

Beyond specific questions within the EAW framework, the *Dorobantu* case is important because it deals with general questions on the relationship between the Charter and the ECHR if minimum requirements have not been developed by the European Union.

Although the main lines of argument as regards the interpretation of the absolute right not to be treated in an inhuman or degrading way have mainly been clarified by the "*Generalstaatsanwaltschaft*" case ("Arranyosi III"); the *Dorobantu* case gave the CJEU the opportunity to specify its "real risk" doctrine as regards possible infringements of Art. 4 of the Charter in detention condition cases. Nonetheless, the judgment left open how to assess factors of single-occupancy cells (TW).

CJEU: EAWs Issued from Austrian Public Prosecutor's Office Valid

After the CJEU decided on 27 May 2019 that the German public prosecution offices lack independence to issue European Arrest Warrants (see joined cases C-508/18 (O.G.) & C-82/19 PPU (P.I.), eucrim 1/2019, pp. 31–33), the CJEU came to a different result as regards the Austrian public prosecutor's offices in a judgment of 9 October 2019. In the case at issue (case C-489/19 PPU), the *Kammergericht Berlin* had doubts whether – following the judgment of May – it could accept EAWs from Austria, because Austrian public prosecutors are subject to discretion or instruction from the executive, i.e., the Austrian Federal Minister of Justice.

The CJEU sees one main difference to the German situation. Under Austrian law, the public prosecutor's decision to issue a national arrest warrant and to issue an EAW must be endorsed by a court before their transmission. In the absence of endorsement, the arrest warrants do not produce legal effects and cannot be transmitted. If the following additional conditions are met, the concept of "issuing judicial authority" in Art. 6(1) of the EAW Framework Decision can be affirmed:
- The court's review of the public prosecutor's decision is ex officio, independent, and objective;
- The court has access to the entire criminal file to which any specific directions or instructions from the executive are added;
- The court is able to review the conditions of issue and the proportionality of the arrest warrants, thus adopting an autonomous decision which gives them their final form.

According to the CJEU, the Austrian law and procedure fulfil all these criteria. Nonetheless, the decision on the German public prosecution offices triggered several uncertainties. Additional references for preliminary rulings on the independence of other EU Member State's public prosecution offices in the EAW context are pending (see also eucrim 2/2019, p. 110). (TW)

Statistics on Use of EAW in 2017

On 28 August 2019, the Commission published statistical data on the use of the European Arrest Warrant in 2017. The document, officially entitled "Replies to questionnaire on quantitative information on the practical operation of the European arrest warrant –Year 2017," compiles data from the EU Member States, both as regards the issuing and the execution of EAWs. The Commission also provides an infographic that outlines the results. In addition, the Commission published a factsheet for citizens entitled "European arrest warrant – Makes Europe a safer place."

As regards Member States as issuing States, the following figures are of interest:

- The total number of EAWs issued by Member States for the year 2017 is 17,491, whereas 16,636 EAWs were issued in 2016 and 16,144 in 2015;
- Most EAWs were issued for theft offences and criminal damage (2649), fraud and corruption offences (1538), and drug offences (1535) in 2017. All these figures indicate a slight increase in comparison to 2016. 241 EAWs were issued for terrorism offences, of which 183 were issued by France alone and 30 by Italy. In comparison, in 2016, 165 EAWs were issued for terrorism offences;
- 6317 issued EAWs resulted in the effective surrender of the person sought in 2017.

As regards Member States as executing States, the following can be said:

- The total number of persons actually arrested in 2017 was 7738, compared to 7056 persons arrested by means of an EAW in 2016 (though only 24 Member States provided information for that year, but 28 for 2017);
- The highest number of arrests in 2017 occurred in the United Kingdom (1510 arrests), Romania (853), and Spain (818);
- In the 26 Member States that provided specific figures, judicial authorities initiated 8801 surrender proceedings;
- The average duration of the extradition procedure – if the person sought did not consent to his/her surrender – decreased from 50.4 days in 2016 to 40.13 days in 2017;
- According to replies from 24 Member States, the execution of an EAW was refused in 796 cases in 2017. This figure is quite stable compared to 2016 (719 refusals for 25 Member States);
- The most common reason for non-execution in 2017 was that contained in Art. 4 No. 6 of the FD EAW: the executing state undertakes the execution of a custodial sentence against its nationals or residents. The situation in 2016 was similar;
- The grounds for mandatory non-execution (Art. 3 of the FD) are still rarely applied;
- Seven Member States reported a total of 100 refusals because the requirements of Art. 4a of the FD EAW (in absentia situations) had not been met in 2017; this is an increase compared to 2016 (65 refusals);
- Fundamental rights issues led to refusals in seven Member States in a total of 109 reported cases.

It should be stressed that the figures must be interpreted cautiously. Not all of the Member States provided replies to every question in the standard questionnaire. Comparison to previous years is even more difficult because the response rates of Member States vary from year to year, and approaches to collecting statistical data vary. (TW)

European Investigation Order

First CJEU Judgment on European Investigation Order

On 24 October 2019, the CJEU delivered its first judgment interpreting Directive 2014/41/EU regarding the European Investigation Order in criminal matters (Case C-324/17 – *Ivan Gazanozov*). The case at issue dealt with the particularity of Bulgarian law that does not provide for any legal remedy against decisions ordering the search, seizure, and hearing of witnesses through a European Investigation Order. The referring Specialised Criminal Court, in essence, wanted to know whether the Bulgarian legislation, which (directly and indirectly) precludes a challenge to the substantive grounds of a court decision issuing an EIO, is in line with Art. 14 of the Directive (for the reference and the opinion of Advocate General *Yves Bot*, see eucrim 1/2019, pp. 36–37).

The judges in Luxembourg decided to reformulate the question referred to and clarified that the referring court is actually uncertain as to how to complete Section J of the form set out in Annex A to the Directive, which is entitled "Legal remedies." In this context, the CJEU stated that a description of the legal remedy must be included only if a legal remedy has been sought against an EIO. It is not necessary to include an abstract description of the legal remedies, if any, that are available in the issuing Member States against the issuing of an EIO. The CJEU is of the opinion that this interpretation results from the wording of Section J of the form in the Annex of the Directive as well as from the objectives pursued by the Directive.

➤ *Put in focus:*

The CJEU's answer can be considered disappointing in view of the protection of defence rights. The judges in Luxembourg did not follow the more far-reaching opinion of the Advocate General. He had concluded that Art. 14 of the EIO Directive not only obliges the Member State to install legal remedies, which enable concerned persons to challenge the substantive reasons for issuing the EIO, but the use of the EIO by that Member State must be frozen until the respective legislation on legal remedies is in place. The CJEU actually reduced the dispute in the main proceedings to a mere formal question. According to the CJEU, it is not necessary to interpret Art. 14 "in the present case." Thus, it implicitly backed the Bulgarian legislation, which does not foresee any legal remedy against the issuance of the EIO – to the detriment of the accused's rights. (TW)

Law Enforcement Cooperation

E-Evidence: Start of Negotiations on EU-US Agreement

On 26 September 2019, the European Commission announced the start of formal negotiations with the United States Department of Justice on an EU-US agreement to facilitate access to electronic evidence in criminal investigations. Both parties reaffirmed their inten-

tion to conclude an agreement as quickly as possible. The next EU-US Justice and Home Affairs Ministerial meeting in December 2019 will review progress. At its meeting on 6 June 2019, the JHA Council endorsed a mandate for the Commission to start negotiations for an international e-evidence agreement with the United States (see eucrim 2/2019, p. 113).

The USA has a negotiating mandate through the CLOUD (Clarifying Lawful Overseas Use of Data) Act of March 2018, which provides criteria for the negotiation of international agreements to facilitate the ability of other countries/partners to obtain electronic data relating to the prevention, detection, investigation, and prosecution of serious crime (for the CLOUD Act, see eucrim 2/2019, pp. 113–114 and the article by *J Daskal* in eucrim 4/2018, pp. 220–225).

On 6 November 2019, the Commission services reported on the second negotiation round. The report reveals that there are still several matters of dispute. The Commission stressed that an EU–US Agreement can only be concluded following agreement on internal EU rules on e-evidence. The Commission also expressed its unhappiness with the UK-US agreement on access to electronic data for the purpose of countering serious crime signed on 3 October 2019.

Other problematic issues included:

- Different definition of data categories in European and American law;
- Types of offences for which data exchange should become possible;
- Involvement of judicial authorities in cross-border orders for e-evidence;
- Definition of service providers and types of service providers to be covered by the agreement;
- The need for strong privacy, data protection, and procedural rights safeguards.

The third negotiating round took place in Washington on 10 December 2019, the day before the EU-US JHA Ministerial meeting. (TW)

MEPs Critical of EU-US E-Evidence Negotiations

At a hearing on 7 November 2019 at the EP's LIBE Committee, MEPs called for meeting EU data protection standards within the framework of possible future data exchanges by means of the U.S. CLOUD Act. The CLOUD Act allows U.S. law enforcement authorities to request the disclosure of data by service providers in the USA, regardless of where the data is stored (for details, see eucrim 1/2018, p. 36; 4/18 p. 207 and the article by *J Daskal* in eucrim 4/2018, pp. 220–225).

The Commission is currently negotiating an agreement by means of which law enforcement authorities in the EU Member States can also benefit from facilitated access to data held by U.S. service providers, such as Microsoft, Facebook, Apple, and Google. The European Data Protection Supervisor *Wiewiórowski* stressed that data can only be transferred for the purpose of a concrete criminal investigation, and he called on the EU Member States to provide efficient remedies against the obligation to data transfers.

MEPs pointed out the much lower data protection standards in the USA and criticised that EP's positions have not yet been taken into account during the negotiations. In addition, MEPs referred to the existing EU-US MLA agreement. (TW)

US and UK Sign Bilateral E-Evidence Agreement

On 3 October 2019, the United States and the United Kingdom signed the first agreement allowing the other party's law enforcement authorities, when armed with appropriate court authorisation, to go directly to tech companies based in the other country to access electronic data in order to combat serious criminal offences. Such agreements are foreseen in the U.S. CLOUD Act, which responds to the converse problem that foreign countries face with respect to their ability to access data held by U.S. service providers (for details, see the article by *J Daskal* in eucrim 4/2018, pp. 220–225).

According to the press release, "[b]oth governments agreed to terms which broadly lift restrictions for a broad class of investigations, not targeting residents of the other country, and assure providers that disclosures through the Agreement are compatible with data protection laws." The other party's permission is required if essential state interests are at stake; this especially concerns death penalty prosecutions by the United States and UK cases involving the freedom of speech.

The agreement was described as "landmark" and "historic" upon its signing. The agreement was signed by U.S. Attorney General *William P. Barr* and UK Home Secretary *Priti Patel* at a ceremony at the British Ambassador's residence in Washington, D.C. The agreement is still in the legislative pipeline. It must be reviewed and approved by the U.S. and UK's parliaments.

The major advantage of the agreement is seen in the acceleration of criminal investigations because law enforcement authorities will no longer need to go through the time-consuming, government-to-government mutual legal assistance process. (TW)

NGOs Urge U.S. Congress to Oppose US-UK CLOUD Act Agreement

On 29 October 2019, twenty privacy, civil liberties, and human rights organizations jointly addressed U.S. Congress committee chairmen to stop the US-UK CLOUD Act Executive Agreement signed on 3 October 2019. It will allow direct access by the party's law enforcement bodies to personal data held by private service providers outside traditional mutual legal assistance procedures.

The organisations "believe that the Agreement fails to adequately protect the privacy and due process rights of U.S. and U.K. citizens." They urge the U.S. parliament to disapprove the agreement.

The organisations observe that the US-UK executive agreement exhibits many often cited human rights concerns, e.g., diminished standards for law enforcement requests, lack of notice, vague oversight mechanisms, etc. They are particularly concerned because the agreement may become a template for future agreements, including with countries that have even less strict data protection standards. The main critical issues put forward are as follows:

- The US-UK Agreement lowers the bar for law enforcement access to both stored communications content, such as emails, and live wiretaps in the USA;
- It does not consistently foresee prior judicial authorization of an order and goes below standards of the Fourth Amendment;
- Requirements for minimization of data and targeting individual requests do not apply equally to the USA and the UK;
- The accord includes neither provisions on notice to the data subject nor any new remedies for individuals;
- The threshold for crimes covered by the agreement is low, and the protective requirement of dual criminality no longer plays a role;
- Vague external oversight;
- The agreement does away with a robust human rights review by the U.S. authorities;
- It also fails to uphold the standards against infringements to the freedom of speech as defined in the CLOUD Act;
- Sharing of gained information among the UK and American law enforcement authorities may violate U.S. law.
- In addition, the undersigning organisations question whether the UK – still a Member of the European Union – was competent to enter into a bilateral agreement. (TW)

EP Report on EU E-Evidence Legislation Advocates Strengthened Safeguards

After the EP elections, the EP Conference of Presidents decided in October 2019 that work should resume on the EU e-evidence rules. The e-evidence package consists of two proposals tabled by the European Commission in April 2018 (see eucrim 1/2018, pp. 35–36): a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

German MEP *Birgit Sippel* (S&D) was reappointed as rapporteur on 4 September 2019. On 11 November 2019, *Sippel* presented her draft report at the LIBE meeting. She proposes a total of 267 amendments, the main proposals of which are as follows:

- Introducing an automatic, meaningful notification of the enforcing EU Member State: the issuing authority must send each Production and Preservation Order not only to the service provider, but also simultaneously to the executing State where the service provider is established or, for service providers not established in the Member States bound by this Regulation, where its legal representative has been appointed;
- Involving the "affected state": not only the "issuing" and "executing" states are part of the procedure, but also the "affected state," i.e., the state of permanent residence of the person concerned. It will have the possibility to bring its doubts as regards the lawfulness of an order to the attention of the executing State;
- Introducing a new refusal mechanism: the draft report introduces several grounds for non-recognition and non-execution of a European Production or Preservation Order. They are aligned to the grounds for refusal provided for in the Directive on the European Investigation Order, thus ensuring consistency. The responsibility for applying these refusal grounds shifts from the service provider to the executing authority, which will now be entitled to refuse the orders based on a list of specific and limited grounds. If the executing authority does not react within a fixed period of time, the service provider is obliged to preserve or produce the requested data to the issuing authority;
- Overhauling the concept of a Regulation and Directive: Sippel suggests directly integrating the content of the proposed Directive into the Regulation, thus clarifying that the providers' obligation to appoint legal representatives cannot be used for other instruments and that the obligation only applies to the Member States participating at the Regulation;
- Obligations in relation to the nomination of legal representatives: the draft report also clarifies that only service providers not established in the EU or EU service providers established in an EU Member State not bound by the Regulation but offering services in the participating Member States are required to designate a legal representative in one of the participating Member States where it offers its services. Regarding service providers already established in a participating Member State, orders should be directly addressed to the main establishment of the service provider where the data controller is established;
- Implementing new review procedure in case of conflicting obligations with third-country law: the report suggests a new review procedure if questions of conflicts of law in third countries (e.g., the USA) arise. By contrast to the Commission proposal, the procedure is more pared down and involves the executing and affected states;
- Reinforcing safeguards for persons concerned: the rights of persons whose data are to be obtained by an order are strengthened and clarified. This includes fairer conditions for issuing orders and clear data categories (based on existing EU and national legislation and in line with CJEU case law). Furthermore, the rapporteur proposes more comprehensive user information, limitations to the use of data obtained, rules on admissibility of evidence and erasure of data obtained, as well as effective legal remedies.

The decision of the LIBE Committee on the draft report is necessary before the suggested amendments can be put forward to the plenary. If the plenary adopts the committee report, trilogue negotiations can start with the Council and the Commission. The Council published a consolidated version of its general approach, including the desired modification to the Commission proposal, on 11 June 2019. (TW)

EDPS Opinion on E-Evidence Proposal

On 6 November 2019, the European Data Protection Supervisor (EDPS) issued his opinion on the new EU legal framework for gathering e-evidence in cross-border cases (for the Commission proposal, see eucrim 1/2018, pp. 35–36).

The EDPS endorses the objective of ensuring quick and effective access of law enforcement to electronically stored data in another state, but calls on the EU legislator to find a balanced approach respecting the Charter of Fundamental Rights of the EU and EU data protection law and implementing all necessary safeguards. The main suggestion in the opinion is to systematically involve judicial authorities of the enforcing Member State as early as possible. These authorities should then have the possibility to effectively and efficiently review compliance of the Production and Preservation Orders with the Charter and to raise grounds for refusal. This view is shared by many civil society stakeholders as well as by the European Parliament (see, e.g., eucrim 1/2019, pp. 38–40).

Furthermore, the EDPS is critical of the definition of the data categories and their overlap, which is not consistent with other EU law. He also calls for a re-balancing between the types of data for which European Production Orders could be issued and the categories of data concerned. The EDPS, in particular, believes that the proposed threshold for producing transactional and content data (three-year minimum of the maximum custodial sentence) is too low. Calling to mind the CJEU case law, which indicates that these data would enable precise profiles of individuals to be established, access can be made possible for serious crime only. The EDPS further argues that the sensitivity of subscriber and access data should not be underestimated because they may include privacy-invasive electronic communications metadata.

The EDPS makes concrete recommendations on the following other issues:

- Data security;
- Rights of the data subject, including enhanced transparency, and rights to remedy;
- Immunities and privileges;
- Legal representatives;
- Time limits to produce data;
- Possibilities for service providers to object.

Ultimately, the EDPS asks for more clarity on the interaction between the EU's internal e-evidence rules and other instruments, especially a future EU-US agreement. In this context, the EDPS stresses that the EU legal framework must uphold a high level of data protection and constitute the reference for respect for fundamental rights when negotiating international agreements on cross-border access to electronic evidence.

The EDPS already issued detailed advice to the Commission regarding negotiations with the USA on an e-evidence agreement (eucrim 1/2019, p. 41). The present opinion also completes other data protection statements, e.g., those by the European Data Protection Board (see eucrim 3/2018, p. 162). (TW)

Council of Europe*

Reported by Dr. András Csúri (AC) and Christine Götz (CG)

Foundations

European Court of Human Rights

Seibert-Fohr New German Judge to ECtHR

The Council of Europe Parliamentary Assembly (PACE) elected Professor *Anja Seibert-Fohr* as new judge to the European Court of Human Rights on 27 July 2019. Her term of nine years commenced on 1 January 2020. Professor *Anja Seibert-Fohr* succeeds Professor *Angelika Nußberger* who has been serving as judge at the European Court of Human Rights for Germany since 2011. *Seibert-Fohr* was a member of the Human Rights Committee from 2013 to 2017. Since 2016, she has held the chair of Public Law, International Law and Human Rights at the University of Heidelberg. (CG)

Specific Areas of Crime

Corruption

GRECO: Fifth Round Evaluation Report on Spain

On 13 November 2019, GRECO published its fifth round evaluation report on Spain. The focus of this evaluation round