



## European Union

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

### Foundations

#### Fundamental Rights

##### Threat of Rule of Law in Poland – Recent Developments

**spot light** New actions and regulations initiated by the Polish ruling party to push through reforms in the justice system triggered further controversies between the country and European institutions/civil society organisations. An overview of the main recent events:

- 19 November 2019: The CJEU rules on the independence and impartiality of the new Disciplinary Chamber at the Polish Supreme Court, considering that the referring court may disapply national legislation if the body to which jurisdiction was conferred to hear a case where the EU law may be applied, does not meet the requirements of independence and impartiality (see details in [eucrim 3/2019, pp. 155–156.](#))
- 5 December 2019: The Labour Chamber of the Supreme Court concludes that the Disciplinary Chamber did not fulfil the requirements of an independent and impartial tribunal. Despite this judg-

ment, the Disciplinary Chamber continued its activities.

- 11 January 2020: Thousands of people, including judges and lawyers from many EU Member States, [assemble for a march through Warsaw](#), in order to protest plans by the Polish government and ruling majority in parliament to discipline the judiciary in Poland. The event was tagged as “1,000 Robes March.”
- 16 January 2020: The European Parliament [adopts a resolution on the Art. 7 procedures against Poland and Hungary](#). It, inter alia, “notes with concern that the reports and statements by the Commission and international bodies, such as the UN, OSCE and the Council of Europe, indicate that the situation in both Poland and Hungary has deteriorated since the triggering of Article 7(1) of the TEU.” The resolution also criticizes the fact that the current Art. 7 procedure and the hearing conducted have not resulted in any significant progress by the two states. MEPs reiterate the need for a new EU mechanism on democracy, the rule of law and fundamental rights (see [eucrim 1/2019, p. 3](#)). Support is again given to the [proposed regulation](#) on the protection of the Union’s financial inter-

ests in case generalized deficiencies as regards the rule of law in Member States occur.

- 21 January 2020: The deputy discipline officer [initiates first disciplinary proceedings](#) against Polish judges having participated in the 1,000 Robes March.
- 23 January 2020: [Poland’s Supreme Court said rulings](#) made by judges appointed under new government rules (affecting several hundred judges) could be challenged, resulting in a number of cases being postponed. The Supreme Court followed the lines of argument given by the CJEU.
- 23 January 2020: The Polish justice ministry – controlled by the ruling PIS party – reacts and declares that the Supreme Court’s judgment has no legal effects.
- 23 January 2020: The lower house of the Polish parliament (the Sejm) [passes a bill introducing further amendments into the Polish judiciary system](#), despite rejection by the opposition-controlled Senate and [criticism by the CoE Venice Commission](#) (opinion of 16 January 2020). The amendments (already initiated in December 2019) included, inter alia, the prohibition of political activities for judges in addition to new disciplinary offences and sanctions for judges and court presidents. Furthermore, the bill declared that any person appointed by the President of the Republic is a lawful judge, and it is prohibited to question his/her legitimacy. Doing so is a disci-

\* If not stated otherwise, the news in the following sections cover the period 1 January – 31 March 2020. Have also a look at the [eucrim homepage \(https://eucrim.eu\)](#) where all news have been published beforehand.

plinary offence, potentially punishable with dismissal. Only the Extraordinary Chamber can decide whether a judge is independent and impartial. The Venice Commission stated in this context: “The [amendment bill] seems to be to make it impossible for any court (...) to question the legitimacy of any court established in accordance with the current legislation.” In the press, the law has been labelled “gagging bill” and “muzzle law.”

■ 28 January 2020: [The Constitutional Tribunal suspends the Supreme Court’s resolution](#) of 23 January 2020. The Constitutional Tribunal declared, inter alia, that the Supreme Court could not limit the adjudication of judges appointed to office by the President of the Polish Republic. Judgments issued by benches which included said judges are binding.

■ 28 January 2020: The Parliamentary Assembly of the Council of Europe ([PACE](#)) [votes to open a monitoring procedure for Poland](#) over the functioning of its democratic institutions and the rule of law. [The resolution](#) declares that recent reforms “severely damage the independence of the judiciary and the rule of law.” PACE called on the Polish authorities to “revisit the total reform package for the judiciary and amend the relevant legislation and practice in line with Council of Europe recommendations.” The Assembly also called on all CoE Member States to ensure that the courts under their jurisdiction ascertain in all relevant criminal and civil cases – including with regard to European Arrest Warrants – whether fair legal proceedings in Poland, as defined under Art. 6 ECHR, can be guaranteed for the defendants. Poland is the first EU Member State to which the CoE monitoring procedure is being applied. The country shares this position with eight other CoE (but non-EU-) Member States, among them Russia, Turkey, and Ukraine.

■ 30 January 2020: The [CCBE publishes a statement on Poland](#) in which the lawyers’ organisation shares the criticism voiced by independent international bodies and organisations in reaction

to the muzzle law. The statement calls on the Polish authorities not to proceed with the law.

■ 10 February 2020: 22 retired judges of the Constitutional Tribunal (including eight former presidents and vice-presidents) [issue an open letter](#) in which they note that the Constitutional Tribunal “has virtually been abolished.” They regret that the actions of the legislature and the executive since 2015 and the Constitutional Tribunal leadership since 2017, “have led to a dramatic decline in the significance and the prestige of this constitutional body, as well as to the inability to perform its constitutional tasks and duties.” The open letter also deals with the pending dispute on the Supreme Court resolution of 23 January 2020, particularly the participation of two former MPs in the bench, that compromise the Constitutional Tribunal’s independence.

■ 11 February 2020: Following the EP resolution of 16 January 2020, [the plenary of the EP again discusses](#) the situation on the rule-of-law threat in Poland. At the beginning, Commission Vice-President [Věra Jourová](#) informed MEPs on the current developments, and Justice Commissioner [Didier Reynders](#) stressed that the Commission will apply all tools at its disposal to maintain the rule-of-law values in Poland. MEPs called on the Commission to take strong action against Poland. German MEP Katarina Barley (S&D) pointed out that Polish judges are in the unbearable situation of facing disciplinary sanctions if they apply EU law. She referred to concrete cases of recent repressions against judges.

■ 14 February 2020: [The “Muzzle Act” \(see above\) enters into force](#). Polish President [Andrzej Duda](#) signed the Act on 4 February 2020 despite continuing [protests](#) voiced by the European Commission, the Council of Europe, and civil society organisations.

■ 17 February 2020: In an unprecedented decision, the [Higher Regional Court of Karlsruhe suspends the execution of a European Arrest Warrant](#) issued

by Poland, because the enacted muzzle law does not guarantee the defendant a fair trial. Although the German court sent a catalogue of questions on the independence of the judiciary in Poland, it released the requested person based on the “high probability” that extradition would be unlawful at the moment (for more details on the decision, see the news in the category “European Arrest Warrant”).

■ 24 February 2020: The President of GRECO, [Marin Mrčela](#), [addresses a letter to the Polish Minister of Justice](#) in which he calls on the Polish government to revise the muzzle law. [Mrčela](#) points out that the diminishing independence of justice may facilitate corruption. He also fully shares the critical opinion of the Venice Commission of 16 January 2020 on the draft bill of the muzzle law.

■ 29 February 2020: The Association of Polish Judges “Iustitia” and association of prosecutors “Lex Super Omnia” publish an extensive [report detailing repressions](#) against Polish judges and prosecutors between 2015 and 2019. The report not only presents information on the investigations and disciplinary proceedings. It also refers to “soft repressions,” consisting, among other things, in the exercise of powers vested in court presidents, which bear features of harassment or mobbing. The report is to be completed with further cases in the future.

■ 9 March 2020: Several experts specialised in the rule of law address an [open letter to Commission President Ursula von der Leyen](#). They criticized the European Commission for being too inactive and lenient towards Poland. Regarding the recent changes implemented by the muzzle law, the experts urge the Commission to take immediate action. This must include expedited infringement action against the muzzle law, and requests for additional interim measures to prevent the muzzle law from being enforced by connecting these measures to the already pending infringement action with respect to Poland’s new disciplinary regime for judges. The Com-

mission should also tackle the rigging of rules as regards the selection of the next president of the Supreme Court, the changes at the Constitutional Tribunal, and the establishment of the National Council of the Judiciary.

■ 26 March 2020: The Grand Chamber of the CJEU declares references for a preliminary ruling of two Polish district courts inadmissible, expressing doubt as to the compatibility of the new disciplinary regime introduced in Poland via judicial reforms in 2017 with Art. 19(1) subpara. 2 TEU ([Joined Cases C-558/18 and C-563/18 – Miasto Łowicz and Prokurator Generalny](#)). The CJEU follows the opinion of AG Tanchev of 24 September 2019 (see [eucrim 3/2019, p. 157](#)). The questions referred are general in nature, because they did not show a connecting factor between the dispute in the main proceedings and a provision of EU law for which interpretation is sought. In essence, the referring Polish judges sought a statement from the CJEU that the disciplinary procedures are a means of ousting judges if they take decisions that do not suit the legislative and executive branches. The CJEU clarified that the concept of preliminary rulings in Art. 267 TEU does not follow this purpose. The Grand Chamber clearly stated, however, that provisions of national law which expose national judges to disciplinary proceedings as a result of the fact that they submitted a reference to the Court for a preliminary ruling cannot be permitted. It is a key element of judicial independence that judges not be subjected to disciplinary proceedings/measures for having exercised their discretion to bring a matter before the CJEU.

■ 8 April 2020: The CJEU [grants the Commission’s application for interim measures](#) against the powers of the Disciplinary Chamber of the Supreme Court with regard to disciplinary cases concerning judges. The powers are based on a 2017 judicial reform. The CJEU requests that Poland suspend the application of the relevant national

provisions before its final judgment on the substance of the case ([C-791/19](#)). The final judgment will be delivered at a later date. The judges in Luxembourg point out that, although the organisation of justice falls within the competence of the Member States, disciplinary regimes applicable to national courts are part of the system of the legal remedies in the fields covered by EU law. Therefore, they must comply with the Union’s requirements on the independence of the judiciary. The mere prospect of Supreme Court judges or judges of the ordinary courts being the subject of disciplinary proceedings that may be referred to a body whose independence is not guaranteed is likely to affect judicial independence. By means of this line of argument, the CJEU confirms the condition of urgency, which is required for granting interim relief. The lack of independence of the disciplinary chamber may cause serious and irreparable harm to the EU legal order.

■ 29 April 2020: The European Commission [launches a new infringement procedure against Poland](#) regarding the muzzle law that entered into force on 14 February 2020 (see above). The Commission concludes in its letter of formal notice that several elements of the new law infringe Union law. This includes the established disciplinary regime that could be used as political control of the content of judicial decisions, thus violating Arts. 19, 47 CFR, which establish the right to an effective remedy before an independent and impartial court. In addition, several elements of the new law do not comply with the principle of the primacy of EU law. In this context, the Commission points out that the law prevents Polish courts from fulfilling their obligation to apply EU law or request preliminary rulings from the CJEU and from assessing the power to adjudicate cases by other judges. Ultimately, the new law is incompatible with the right to respect for private life and the right to the protection of personal data as guaranteed by the CFR and the GDPR, since

it requires judges to disclose specific information about their non-professional activities. The Polish government now has two months to reply to the letter of formal notice.

■ 25 May 2020: At a [meeting of the LIBE Committee](#), MEP *Juan Fernando López Aguilar* (S&D, ES) presents a [draft interim report](#) that serves as a basis for an EP resolution on the way forward as regards the Article 7 procedure against Poland that was triggered by the European Commission in December 2017. The report (1) takes stock of the developments as regards the rule of law, democracy, and fundamental rights in Poland since 2015; and (2) urges the Commission and the Council to widen the scope of the Article 7(1) TEU procedure to include an assessment of clear risks of serious breaches of democracy and fundamental rights. During the discussions, most MEPs shared concerns over the systematic and continuing attacks against judicial independence and democratic institutions in Poland. They called on the Council and Commission to take decisive actions against Poland, including budgetary measures. The President of the European Association of Judges and a representative of the Polish judges association *Iustitia* reported on concrete examples of violations of judicial independence and disciplinary proceedings against Polish judges. They called for a “European Marshall Plan” to uphold the EU’s core values in Poland. The plenary of the EP is to vote on the proposed resolution in September 2020. (TW)

#### Rule-of-Law Developments in Hungary

**spot light** Although the executive attacks on the independence of the judiciary in Poland dominate headlines in the media, European institutions also have rule-of-law concerns with regard to Hungary. Next to Poland, Hungary is subject to an Article 7 TEU procedure, which may eventually lead to sanctions against an EU Member State if the Council states a clear risk of a seri-

ous breach of EU values. The procedure against Hungary was triggered by the European Parliament in September 2018. Concerns mainly address judicial independence, freedom of expression, corruption, rights of minorities, and the situation of migrants and refugees. As in the case of Poland, Hungary faces several infringement actions before the CJEU. The recent developments in brief:

- 14 January 2020: [Advocate General Campos Sánchez-Bordona proposes](#) that the CJEU declares Hungarian legislation imposing restrictions on the financing of civil organisations from abroad to be incompatible with EU law. The Hungarian legislation imposes several obligations of registering, providing certain pieces of information and publication on civil organisations if they receive donations above a certain threshold from abroad. The case was brought to the CJEU in an infringement action by the Commission ([Case C-78/18](#)). The AG argues that the legislation is contrary to the principle of free movement of capital in that it includes provisions amounting to unjustified interference with the fundamental rights of respect for private life, protection of personal data, and freedom of association as protected by the Charter. Objectives, such as the protection of public policy and the fight against money laundering and terrorist financing, cannot justify the Hungarian legislation.
- 16 January 2020: The European Parliament notes in a [resolution on the ongoing Article 7 procedures](#) against Poland and Hungary that reports and statements by the Commission, the UN, OSCE, and the Council of Europe indicate that “the situation in both Poland and Hungary has deteriorated since the triggering of Article 7(1).” MEPs expressed their dissatisfaction on the hearings within the Council; they have not yet resulted in any significant progress. The resolution states that “the failure by the Council to make effective use of Article 7 of the TEU continues to undermine the integrity of common European values, mutual trust, and the credibility of the Union as

a whole.” The Council is called on to determine the existence of a clear risk of Hungary’s serious breach of the values on which the Union is founded. The EP also criticizes the modalities of the procedure and shortcomings in the proper involvement of the EP in the Article 7 procedure.

- 5 March 2020: In other infringement proceedings ([Case C-66/18](#)), Advocate General [Juliane Kokott voices her belief](#) that the 2017 amendments of the Hungarian law on Higher Education do not comply with EU and WTO law. The amendment stipulates that higher education institutions from countries outside the European Economic Area would only be allowed to continue their activities in Hungary if an international treaty existed between Hungary and their home country. In addition, the new rules require foreign universities to operate in their country of origin if they want to offer higher education in Hungary. The law was seen as a move against Hungarian-born US businessman George Soros – an opponent of Hungarian Prime Minister *Viktor Orbán* – because his funded Budapest-based Central European University was the only active foreign higher education institution in Hungary that did not meet the new requirements. According to AG *Kokott*, the new rules are discriminatory and disproportionate; they infringe the freedom of establishment, the Services Directive, the Charter of Fundamental Rights, and the national treatment rule of the General Agreement on Trade in Services (GATS).

- 24 March 2020: Given the plans of the Hungarian government to expand “state of danger” measures due to the COVID-19 pandemic and to rule with executive decrees, the [EP’s Civil Liberties Committee \(LIBE\) issues a reminder](#) that all Member States have a responsibility to respect and protect fundamental rights, the rule of law, and democratic principles, even in difficult times. The chair of the committee, [Juan Fernando López Aguilar \(S&D, ES\)](#), called on the Commission to assess whether the

proposed bill complies with the values enshrined in [Article 2 of the Treaty on European Union](#).

- 30 March 2020: The Hungarian Parliament passes the contentious “state of emergency extension” [bill](#). [The new law](#) (dubbed the “Enabling Act”) gives the national conservative Hungarian government headed by *Viktor Orbán* the right to pass special executive decrees in response to the coronavirus outbreak. It also changes the Hungarian criminal code by introducing jail terms of up to five years for people who spread “fake news” about the virus or measures against it. Severe penalties were also introduced if people breach the quarantine ordered by authorities. For details, see also the [analysis by Renáta Uitz on Verfassungsblog](#). The law was heavily criticized by the opposition, the Council of Europe, and human rights organisations. They mainly disagree with the indefinite term of the expanded state of emergency and fear inappropriate restrictions on the freedom of press and freedom of expression. Another fear is that the “Enabling Act” cements the erosion of the rule of law in Hungary. In a [letter of 24 March 2020](#) to *Viktor Orbán*, CoE Secretary General *Marija Pejčinović Burić* stated, inter alia: “An indefinite and uncontrolled state of emergency cannot guarantee that the basic principles of democracy will be observed and that the emergency measures restricting fundamental human rights are strictly proportionate to the threat which they are supposed to counter.” CoE Human Rights Commissioner *Dunja Mijatović* commented the following on Twitter: “[#COVID19](#) bill T/9790 in [#Hungary’s](#) Parliament would grant sweeping powers to the gov to rule by decree w/o a clear cut-off date & safeguards. Even in an emergency, it is necessary to observe the Constitution, ensure parliamentary & judicial scrutiny & right to information.”

- 15 April 2020: Upon the initiative of Transparency International EU, 30 MEPs and 50 civil society organisations



send an [open letter](#) to the presidents of the European Commission and the Council calling on “swift and decisive actions” against Hungary. The letter eyes the new Hungarian emergency law of 30 March 2020. Although exceptional times during the COVID-19 pandemic “demand exceptional measures and it may be legitimate for governments to temporarily use extraordinary powers to manage the situation,” the latest actions by the Hungarian government are a “flagrant attack on the cornerstones of the rule of law and the values of the Union,” the signatories emphasise. The law of 30 March 2020 has a “chilling effect on free speech and anticipate the potential to suffocate those remaining elements of the checks and balances system in Hungary.”

■ 17 April 2020: In a [resolution on EU coordinated action to combat the COVID-19 pandemic](#) and its consequences, the EP voices deep concern over the steps taken by Hungary to prolong the state of emergency indefinitely, to authorise the government to rule by decree without a time limit, and to weaken the emergency oversight of the parliament. These measures are deemed “totally incompatible with European values.” The Commission is called on to make use of all available EU tools and sanctions to address this serious and persistent breach; the sanctions could include budgetary cuts. The Council is called on to resume the ongoing Article 7 procedures against Hungary.

■ 20 April 2020: 75 European personalities, including former European Commission president *Jean-Claude Juncker*, former heads of state and government, and major figures from European civil society [publish an open letter](#) calling on the EU to swiftly propose and adopt sanctions against the latest “democratic backsliding” by the Hungarian government. The signatories voice concern over the recent drift of *Victor Orban’s* government towards autocracy in Hungary. The emergency law of 30 March 2020 is criticized as an unprecedented concen-

tration of power: “It does not serve the fight against COVID-19 or its economic consequences; instead, it opens the door to all types of abuses, with both public and private assets now at the mercy of an executive that is largely unaccountable,” the letter says. The letter calls on all European stakeholders to get aware of the situation in Hungary and to take collective action. As guardian of the EU Treaties, the Commission is called on to urgently propose sanctions taking into account the seriousness of violation of European rules and values. The EP and Council should adopt these sanctions without delay. National media are advised to dedicate news segments to the Hungarian situation (daily, if necessary) and to grant Hungarian citizens free access to their content as a source of pluralistic and independent information.

■ 7 May 2020: In a [hearing before the Committee on Legal Affairs \(JURI\)](#), Commissioner for Justice and Consumer Affairs, *Didier Reynders*, reiterates that the Commission closely monitors the proportionality of emergency measures taken by the EU Member States during the coronavirus crisis. This includes the Enabling Act in Hungary with its indefinite term of application and its restrictions to the freedom of expression/freedom of press. MEPs are concerned over the situation in countries like Poland and Hungary, which they fear used the crisis to put in place measures that weaken democracy.

■ 14 May 2020: In a plenary debate with European Commission Vice-President *Věra Jourová* and the Croatian Presidency of the EU, [several MEPs reiterate their criticism of the emergency measures](#) taken by the Hungarian government to fight the COVID-19 pandemic. Next to the indefinite state of emergency, MEPs particularly criticise the criminalization of ostensible “fake news,” as it is a measure directed against government-critical statements. MEPs urge the Commission to promptly open infringement procedures against the Hungarian emergency law. Further-

more, EU funding to Hungary should be stopped, unless rule of law is respected. The Council is called on to move forward with the Article 7 procedure initiated by the EP in 2018. (TW) ■

### Bar Associations’ Resolution on Rule of Law

On the occasion of the 48th European Presidents’ Conference on 21 February 2020 in Vienna, representatives from over 50 bar associations adopted [a resolution on the rule of law and the independence of justice](#). European Institutions and national authorities are urged to do the following:

- Make full use of the tools available in order to safeguard and restore the independence of the judiciary and the administration of justice in Europe;
- Maintain the strict autonomy and independence of bar associations and the legal professions, including the judiciary, especially as regards disciplinary proceedings.

In particular, the resolution recommends using expedited infringement procedures and filing applications for interim measures before the CJEU.

The resolution also includes a call to a “March of European Robes” between 24 and 26 June 2020 in Brussels in order to voice, in the heart of Europe, the lawyers’ commitment to the rule of law, the separation of powers, an independent judiciary, and fundamental rights. (TW)

### EU Action Plan on Promotion of Human Rights and Democracy in the World

On 25 March 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) presented their plans for the future EU policy on strengthening human rights and democracy in the EU’s external actions. The package presented to the public consists of the following:

- [Joint Communication EU Action Plan on Human Rights and Democracy 2020–2024](#);
- [EU Action Plan on Human Rights and Democracy 2020–2024](#);

- [Joint Proposal for a recommendation of the Council to the European Council](#) on the adoption of a decision identifying the strategic objectives of the Union to be pursued through the EU Action Plan on Human Rights and Democracy 2020–2024;
- [Annex to the Joint Proposal for a recommendation of the Council to the European Council](#).

The Joint Communication notes that past EU policy achieved significant progress in countries and regions where human rights were under strain; however challenges persist. Among the critical trends listed by the Communication:

- Weakening of the rule of law;
- Increased violence and intimidation of human rights defenders (over 2600 reported attacks over the past three years);
- Widespread impunity for human rights violations and attacks on the role of the International Criminal Court.

In addition, new technologies and global environmental problems, e.g., climate change, pose additional threats to human rights. Against this background, a renewed focus on human rights and democracy is necessary to strengthen state and societal resilience. The Joint Communication proposes the following:

- Enhancing EU leadership in promoting and protecting human rights and democracy worldwide;
- Setting out EU ambitions, identifying priorities, and focusing on implementation in view of changing geopolitics, digital transition, environmental challenges, and climate change;
- Maximising the EU's role on the global stage by expanding the human rights toolbox, its key instruments, and its policies;
- Fostering a united and joined-up EU by promoting more efficient and coherent action.

The EU Action Plan 2020–2024 defines the priorities of the EU and the Member States in their relationship with third countries more concretely. It aims at promoting human rights and democracy consistently and coherently in all

areas of EU external action (e.g., trade, environment, development). In operational terms, the Action Plan has five lines of action that will be implemented on the ground in partner countries:

- Protecting and empowering individuals;
- Building resilient, inclusive, and democratic societies;
- Promoting a global system for human rights and democracy;
- New technologies: harnessing opportunities and addressing challenges;
- Delivering results by working together.

The Action Plan 2020–2024 builds on two previous action plans that were adopted in 2012 and 2015 for a four-year period each. It also takes into account the 2012 [EU strategic framework on human rights and democracy](#).

The accompanying Joint Proposal refers to Art. 22 TEU and invites the European Council to adopt the Action Plan – by unanimity – as a strategic interest of the EU. In the affirmative, decisions on actions implementing the Action Plan could then be taken by qualified majority voting in the Council. This procedure would make the EU more assertive.

The documents are now being transmitted to the Council and the European Parliament. The Council is now called on to adopt the Action Plan and to decide on faster and more efficient decision-making in the area of human rights and democracy. (TW)

## **Area of Freedom, Security and Justice**

### **Brexit – The Way Forward**

At the end of 31 January 2020, the United Kingdom left the European Union. The [“Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community”](#) of October 2019 was endorsed by the Council and the European Parliament. The Withdrawal Agreement

entered into force and started a transition period that will end on 31 December 2020. In essence, the United Kingdom will continue to apply Union law during the transition period but will no longer be represented in the European institutions. The special position of the United Kingdom in respect of measures in the area of freedom, security and justice will also continue. The Joint Committee may, before 1 July 2020, adopt a single decision extending the transition period for up to one or two years.

Ongoing police and judicial cooperation in criminal matters is regulated in Part III, Title V of the Withdrawal Agreement (Art. 62 et seq.). The framework of the future relationship between the European Union and the United Kingdom is set out in the [Political Declaration of 17 October 2019](#). From the outset, the Political Declaration emphasises the importance of data protection. The EU and the UK are committed to ensuring a high level of personal data protection to facilitate data flows and exchanges, which are seen as key to the future relationship. Part 3 of the Political Declaration outlines the policy objectives of the future security partnership. The partnership will comprise law enforcement and judicial cooperation in criminal matters, foreign policy, security and defence, and thematic cooperation in areas of common interest.

On 25 February 2020, the General Affairs Council [formally authorised](#) the Commission to negotiate a new partnership agreement with the United Kingdom. The Council also adopted [negotiating directives](#) that specify the Commission's mandate for the negotiations. The directives largely follow the recommendation presented by the Commission on 3 February 2020 ([COM\(2020\) 35 final](#)). They mainly build on the aforementioned political declaration of October 2019. The EP already endorsed the draft directives in a [resolution of 12 February 2020](#).

The negotiating directives reiterate the EU's wish to set up an ambitious,

wide-ranging, and balanced economic partnership with the UK. The EU intends to establish a free trade agreement with the UK to ensure that zero tariffs and quotas apply to trade in goods. This agreement regulates customs cooperation and regulatory aspects. The mandate also contains provisions for future cooperation in areas such as digital trade, intellectual property, public procurement, mobility, transport, and energy.

- As regards the envisaged security partnership, the EU reiterates its aim to establish a broad, comprehensive, and balanced security partnership with the UK. As regards future law enforcement and judicial cooperation, in particular, the mandate outlines the following aspects:

- Although the security partnership should provide for close law enforcement and judicial cooperation in relation to the prevention, investigation, detection, and prosecution of criminal offences, account must be taken of the UK's future status as a non-Schengen third country, meaning that the UK cannot enjoy the same rights and benefits as a Member State;

- Respect for fundamental rights, including adequate protection of personal data, is a necessary condition for the envisaged cooperation. The EU will automatically terminate cooperation if the UK no longer gives effect to the ECHR;

- The security partnership must also provide judicial guarantees for a fair trial, including procedural rights, e.g., effective access to a lawyer. Cooperation instruments must lay down appropriate grounds for refusal, including a transnational *ne bis in idem*;

- In the area of data exchange, the security partnership should include PNR arrangements, an information exchange (currently foreseen within the Prüm framework), and the effective/efficient exchange of existing information and intelligence, e.g., on wanted and missing persons/objects;

- Within the framework of operational cooperation, the partnership should provide for cooperation between the UK

and Europol/Eurojust in accordance with Union standards on third country cooperation;

- A streamlined extradition scheme should be built up, which includes the possibility to waive the double criminality check for certain offences, to make arrangements regarding political offences, to give EU Member States the right to not extradite own nationals, and to allow additional guarantees in particular cases;

- In other areas of cooperation in criminal matters, a future agreement should facilitate and supplement the application of relevant CoE conventions; arrangements may impose time limits, foresee standard forms, and must take into account the latest technological advancements;

- The envisaged partnership should include commitments to support international efforts to prevent and fight against money laundering and terrorist financing, which comply with the FATF standards or even go beyond these standards as far as certain aspects are concerned (e.g., beneficial ownership).

Ultimately, the mandate foresees that the future partnership should be embedded in an overall governance framework covering all areas of cooperation. The Commission has a [special website](#) that provides regular updates on the Brexit negotiations. Negotiations on an agreement for the post-transition phase started in early March 2020. The Commission published a [draft text on the new partnership agreement](#) with the UK on 18 March 2020. (TW)

### Commission: White Paper on AI

**spot light** On 19 February 2020, the Commission presented a “[White Paper on Artificial Intelligence: a European approach to excellence and trust](#).” The White Paper outlines policy options on how to achieve the dual objectives of promoting the uptake of artificial intelligence (AI) and addressing the risks associated with certain uses of this new technology.

The Commission sets out that AI will bring a number of benefits to all of European society and economy. Hence, the EU is set to become a global leader in innovation in the data economy and its applications. The Commission, however, also points out that the new technology entails a lot of potential risks in relation to fundamental rights and EU fundamental values, such as non-discrimination. Therefore, any trustworthy and secure development of AI solutions in the future must respect the values and rights of EU citizens, e.g., the rights to privacy and data protection. Against this background, the White Paper identifies two main building blocks:

- “An ecosystem of excellence” that sets out the policy frameworks needed to mobilise the necessary economic resources, including research and innovation and providing the right incentives for small and medium-sized enterprises, in particular;

- “An ecosystem of trust” that sets out the key elements of a future regulatory framework for AI in Europe ensuring compliance with EU rules.

For high-risk cases, e.g., health, policing, justice, and transport, the White Paper suggests that AI systems should be transparent, traceable, and guarantee human oversight. Authorities should be able to test and certify the data involving algorithms used to check cosmetics, cars, or toys.

The Commission wishes to launch a broad public debate in Europe specifically on the gathering and use of biometric data for remote identification purposes, for instance through facial recognition in public places. The debate should focus on how their use can be justified as an exception to the general prohibition of remote biometric identification. It should also focus on which common safeguards need to be established in accordance with EU data protection rules and the Charter of Fundamental Rights. For lower-risk AI applications, the Commission envisages a voluntary labelling scheme if certain defined standards are respected.

Another challenge is whether current EU and national legislation on liability is sufficient to compensate persons who suffered harm from the application of AI technology. According to the Commission, there is currently no need to completely rewrite liability rules. It would like to garner opinions on how best to ensure that safety continues to meet a high standard and that potential victims do not face more difficulties in getting compensation compared to victims of traditional products and services. The liability challenges are identified in more detail in a [“report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics.”](#) The report accompanies the White Paper.

Together with the launch of the White Paper, the Commission opened a [public consultation](#). All European citizens, Member States, and relevant stakeholders (including civil society, industry, and academia) are invited to provide their feedback on the White Paper and on the EU approach to AI by 31 May 2020.

It should also be noted that the White Paper is accompanied by the [European data strategy](#) that was presented on the same day. Both documents are the first pillars of the new [digital strategy](#). The new strategy comes in response to the digital transformation that affects all European citizens and businesses. Under the heading “putting people first and opening new opportunities for business,” the EU has the following digital strategy aims:

- Developing technology that works for the people;
- Ensuring a fair and competitive digital economy;
- Establishing an open, democratic, and sustainable society.

These three pillars were further outlined in the [political guidelines of Commission President Ursula von der Leyen](#), who emphasises that digital transformation must go hand-in-hand with the second main future challenge: the European Green Deal. In this context, during her

first 100 days in office, she kick-started the debate on human and ethical Artificial Intelligence and the use of big data to create wealth for societies and businesses. The Commission [plans further actions](#) as regards the implementation of ideas on the digital world. (TW)

### EP LIBE: AI in Criminal Law

On 20 February 2020, MEPs in the LIBE Committee heard experts on the benefits and risks of artificial intelligence in the criminal law framework. In the hearing [“Artificial Intelligence in Criminal Law and Its Use by the Police and Judicial Authorities in Criminal Matters,”](#) discussion focused on facial recognition, risk assessment, and predictive policing (see also the [hearing agenda](#)). Panelists observed that the use of AI for voice processing is already commonplace. In the future, AI should be increasingly applied in the field of terrorist financing.

As regards the use of AI for biometric facial identification, participants voiced concerns over the risks to fundamental rights. Data quality poses one of the major challenges in this area. Another problem related to the use of AI for facial identification is the so-called algorithmic bias, which may lead to discrimination of ethnic groups. Against this background, participants discussed how the EU can ensure transparency, explainability, and accountability. The existing regulatory framework therefore needs to be adjusted, as proposed by the European Commission in its [White Paper on Artificial Intelligence](#), which was made public on 19 February 2020 (see also separate news item). (TW) ■

### EP: Resolution on Artificial Intelligence and Automated Decision Making

EU institutions are dealing with the question of how the EU should react to the rapid development of artificial intelligence (AI). Alongside the Commission White Paper on AI of 19 February 2020, which was followed by the LIBE committee hearing on the use of AI in the criminal law field (see separate news

items), the European Parliament adopted a [resolution on 12 February 2020](#): the resolution focuses on consumer protection as regards AI technology and automated decision making (ADM). It sets out that an examination of the current EU legal framework, including the consumer law acquis, product safety, and market surveillance legislation, is needed to check whether it is able to properly respond to AI and ADM and provide a high level of consumer protection. MEPs mainly state the following:

- ADM has huge potential to deliver innovative and improved services, but consumers should “be properly informed about how the system functions, about how to reach a human with decision-making powers, and about how the system’s decisions can be checked and corrected”;
- ADM systems should use “explainable and unbiased algorithms”;
- Review structures must be set up to remedy possible mistakes;
- While automated decision-making processes can improve the efficiency and accuracy of services, “humans must always be ultimately responsible for, and able to overrule, decisions that are taken in the context of professional services,” e.g., legal professions;
- Supervision or independent oversight by qualified professionals is important where legitimate public interests are at stake;
- Legislation must follow a risk-based approach.

MEPs favour adjusting the EU’s safety and liability rules to the new technology. The Commission is called on to take respective legislative action.

The resolution will be transmitted to the Council and the Commission, so that they can take the EP’s views on AI into account. Digital transformation is one of the priorities of the Commission under President *Ursula von der Leyen*. (TW)

### CCBE Position Paper on AI

In March 2020, the Council of Bars & Law Societies in Europe (CCBE) pub-



lished a [position paper](#) in which it sets out its considerations on the legal aspects of artificial intelligence (AI). The CCBE voices several concerns over the use of AI in the following areas that directly concern the legal profession:

- AI and human rights;
- The use of AI by courts;
- The use of AI in criminal justice systems;
- Liability issues;
- The impact of AI on legal practice.

The CCBE notes that lawyers should be further involved in future developments of AI, e.g., further studies and reflections at the EU and Council of Europe level, because both access to justice and due process are at stake.

Regarding human rights concerns, the CCBE paper calls on AI developers to act responsibly. This could be framed by ethics codes or new codifications setting out the principles and requirements for the use of AI. In addition, the following is recommended:

- Putting AI systems under independent and expert scrutiny;
- Duly informing persons impacted by the use of an AI system;
- Ensuring the availability of remedies for these persons.

Regarding the use of AI by courts, the CCBE underlines that AI tools must be properly adapted to the justice environment given the risk that access to justice may be undermined by AI tools. Therefore, the following parameters should be taken into account:

- Possibility for all parties involved to identify the use of AI in a case;
- Non-delegation of the judge's decision-making power;
- Possibility to verify the data input and reasoning of the AI tool;
- Possibility to discuss and contest AI outcomes;
- Compliance with GDPR principles;
- The neutrality and objectivity of AI tools used by the judicial system should be guaranteed and verifiable.

The CCBE highlights the sensitivity of the use of AI in the area of criminal

justice. Here, several challenges come to light. Therefore, AI systems should be introduced only when there are sufficient safeguards against any form of bias or discrimination. All measures of increased surveillance should be carefully balanced against the impact they may have on an open and pluralistic society.

AI, however, can also support lawyers and law firms in coping with the increasing amount of data generated. The use of AI by lawyers is more or less limited to research tools, simplification of data analytics and, in some jurisdictions, predicting possible court decisions. Nonetheless, AI will change the work of legal professionals and the way how legal advice is provided. In this context, challenges arise as to the competence of lawyers; they must, for instance, be able to ask meaningful questions about the decisions made by AI, and to point out the limits of applicability and utility of AI systems, which cannot remain in a purely technical domain. This necessitates appropriate training of lawyers.

In the overall conclusions, the CCBE emphasises that with the great opportunities and benefits offered by AI also comes a great responsibility to ensure that AI remains ethical and respects human rights. The use of AI does, in certain aspects, pose significant threats to the quality of our justice systems, the protection of fundamental rights and the rule of law. The development of AI tools must take into account the role and interests of all actors in the justice system. Against this background, one of the main messages of the position paper is that there is a clear need for the CCBE and its membership to continue monitoring the impact of the use of AI in the legal and justice area. (TW)

## Schengen

### COVID-19 Travel Restrictions – Guidance by Commission

On 30 March 2020, the European Commission issued [practical guidance](#) on

implementation of the [temporary restriction on non-essential travel](#) to the EU. The ban pursuant to the Schengen Borders Code was outlined in a Commission Communication of 16 March 2020. The guidance paper issued now aims to assist border guards and visa authorities. It gives advice on implementation of the temporary restriction at the border, on facilitating transit arrangements for the repatriation of EU citizens, and on visa issues. It addresses issues that Member States raised in the bi-weekly videoconferences of Home Affairs Ministers and in technical meetings with Member States.

Frontex, Europol, and the European Centre for Disease Prevention and Control (ECDC) assisted in the preparation of the guidance. It also follows up on the [joint statement](#) of the Members of the European Council of 26 March 2020, which emphasised the need to step up efforts to ensure that EU citizens stranded in third countries who wish to go home can do so. (TW)

## Institutions

### Council

#### Coronavirus Dominates JHA Council Meeting of March 2020

The [first formal JHA Council meeting](#) under the Croatian Presidency on 13 March 2020 was dominated by the coronavirus crisis. Ministers discussed civil protection items, in particular:

- Lessons learnt so far in the tackling of the COVID-19 outbreak;
- Possible additional preparedness and response measures for the EU Civil Protection Mechanism;
- Ways to step up information-sharing, making full use of the integrated political crisis response (IPCR) toolbox;
- Additional support from Member States.

Other topics in relation to the coronavirus included the EU guidelines

for health screening at borders and the working methods of the Council during the crisis.

Ministers also dealt with the strategic guidelines for justice and home affairs, which will further implement the common EU objectives set out in the strategic agenda 2019–2024, as adopted by the EU leaders in June 2019. The Council Presidency observed that despite broad support for the strategic JHA guidelines, agreement could not be reached since two Member States are still opposing. Further consultations will have to take place. (TW)

## European Commission

### Commission Work Programme Published

On 20 January 2020, the Commission published its [Work Programme for the year 2020](#). The first annual Work Programme is entitled “A Union that strives for more” and sets out the most important Commission initiatives in the programme’s first year, including commitments for the first 100 days. The Work Programme is based on [the headline ambitions presented in the Political Guidelines issued by Commission President von der Leyen](#). It reflects the main priorities for the European Parliament and those in the European Council’s Strategic Agenda for 2019–2024.

In the security context, the Work Programme outlines the Commission’s intention to put forward a new Security Union Strategy. This strategy shall define the areas in which the EU can offer added value to support Member States in their efforts to ensure security. Security areas include:

- Combatting terrorism and organised crime;
- Preventing and detecting hybrid threats;
- Cybersecurity;
- Increasing the resilience of critical infrastructure;
- Strengthening Europol’s mandate in

order to reinforce operational police cooperation.

Further priorities in the field of criminal law under the Work Programme include plans for an EU Strategy enabling a more effective fight against child sexual abuse and a new Action Plan on anti-money laundering. (CR)

## European Court of Justice (ECJ)

### Information on Working Arrangements during the COVID-19 Pandemic

On 30 March 2020, the Court of Justice published an [important message for parties](#) to the proceedings with regard to its judicial activities during the coronavirus COVID-19 pandemic. According to the information, judicial activity at the Court of Justice continues, with priority being given to urgent cases. While procedural time limits for instituting proceedings and for lodging appeals continue to run, time limits in ongoing non-urgent proceedings have been extended by one month. Time limits that are to be fixed by the registry shall also be extended by one month. Hearings that were scheduled up until 30 April 2020 have been adjourned until a later date can be arranged.

The General Court of the EU has adjourned all hearings until 3 April 2020, dealing only with particularly urgent cases. When possible, however, it is also endeavouring to continue dealing with other cases. The Courts recommend consulting the website of the [Court of Justice of the EU](#) for regular updates. (CR)

### New Version of Practice Directions Adopted

In February 2020, the Court of Justice adopted a [new version of its Practice Directions](#), containing information on developments regarding the protection of personal data and the handling of appeals.

Data protection rules, for instance, require party representatives to give full

effect in their pleas or written observations to an order – made by the referring court or by the Court of Justice – that data must be anonymous in preliminary ruling proceedings. The same goes for orders made by the General Court in cases of appeals. With regard to appeals at the General Court, the Practice Directions recall that such appeals are limited to questions of law and should not, in principle, reveal secret or confidential information. Another reminder addresses the need to lodge a special request along with the appeal to allow it to proceed in cases of Article 58a of the Protocol on the Statute of the Court of Justice of the EU. Lastly, the Practice Directions draw attention to the importance of complying with formal requirements relating to procedural acts.

As regards the oral stage of procedure, the Directions reiterate the criteria governing the organisation of an oral hearing. Specific guidance is given on arrangements to be made before the hearing, e.g., regarding language requirements, disability, or reduced mobility. (CR)

### New Advocate General Appointed

*Jean Richard de la Tour* has been appointed [Advocate General](#) at the Court of Justice for the period from 23 March 2020 to 6 October 2024. Before joining the Court, Mr *de la Tour* served as First Advocate General of the Commercial, Financial and Economic Chamber of the French Court of Cassation. He replaces former Advocate General *Yves Bot*, who passed away on 9 June 2019. (CR)

## OLAF

### OLAF’s Work in Times of Crisis

On 7 April 2020, OLAF informed the public that it is still fully operational and committed to fighting fraud despite the restrictions set up by the Belgian authorities during the coronavirus crisis. The [press release](#) provides some statistical data on OLAF’s case work

since 16 March 2020. OLAF has also developed specific rules on conducting interviews in times when travelling is not recommended. It points out that the COVID-19 pandemic offers new opportunities for fraudsters to take advantage of the increased demand for medical supplies, personal protection, and hygiene products. In this context, OLAF refers to its successful investigation against fake COVID-19 related products (see separate news item). OLAF investigators and analysts have quickly adapted to the extraordinary situation thanks to secure remote access to OLAF's IT systems and other working tools. (TW)

### OLAF Investigation into Fake COVID-19 Related Products

After the outbreak of the coronavirus in Europe, fraudsters started to benefit from the distress and needs of the population. In March 2019, [OLAF opened an investigation](#) into the import of fake products to be used against the COVID-19 infection: masks, medical devices, disinfectants, sanitisers, and test kits. These products proved to be ineffective, non-compliant with EU standards, and even detrimental to health.

OLAF has been collecting intelligence and information on this type of illicit trafficking since the beginning of the pandemic. It provides customs authorities in the EU Member States and third countries with relevant information in real time. The products entered the EU by means of misdeclarations or fake certificates, black market sales, and smuggling.

On 13 May 2020, OLAF informed of the [progress made as regards its inquiry into the fake COVID-19 products](#). The interim results include:

- Identification of over 340 companies acting as intermediaries or traders of counterfeit or substandard products;
- Seizure of millions of substandard medical products with fake EU conformity certificates in several Member States;
- Establishment of an OLAF Cyber

Task Force comprised of experts specialised in cyber criminality that trawl the internet with the objective of identifying and taking down illicit websites offering fake products;

- Increased identification of ineffective medicine products (e.g., pills);
- Collection of intelligence in order to determine the true origin of face masks, medical devices, disinfectants, sanitisers, medicines, and test kits, which is currently the most pressing challenge in dealing effectively with the fraudulent schemes.

OLAF stressed that close cooperation with all customs and enforcement authorities in the EU and many other countries as well as with international organisations, e.g., Europol, Interpol, the WCO, and EUIPO, has been established. This proved essential to target shipments and identify the fraudulent companies. OLAF also warned that small shipments with fake or substandard products due to direct sales online to European customers by companies based in non-EU countries are posing a major challenge. (TW)

### Successful OLAF Operations Against Smuggling

In February 2020, OLAF informed the public about several successful actions against illicit trade and trafficking:

- With the support of OLAF, Belgian and Malaysian customs authorities were able to [seize a record sum of nearly 200 million smuggled cigarettes](#). After the Belgian authorities successfully seized around 135 million cigarettes in Antwerp, OLAF launched an investigation against the smugglers and the routing. Over 62,6 million cigarettes had been falsely declared and were waiting for export from a free trade zone in Malaysia. After having been alerted by OLAF, the Malaysian authorities seized the containers on 3 February 2020, preventing the cigarettes from being shipped to the EU. If the cigarettes had been successfully brought to the markets in the EU, OLAF estimates that financial loss to the

EU/Member State budgets would have been €50 million.

- In close cooperation with OLAF, the Italian Customs Agency [seized 12.5 tonnes of fluorinated greenhouse gases](#), so-called hydrofluorocarbons (HFCs), on 5–6 February 2020. HFCs replace ozone-depleting substances and are often used in refrigerated units. Although they do not deplete the ozone layer, they have a high global warming potential. The illicit import of such gases became one of OLAF's operational priorities, in line with the top priority on the agenda of the new Commission under *Ursula von der Leyen*, who announced plans to make Europe the first climate neutral continent by 2050: “The European Green Deal.”

- On 12 February 2020, OLAF reported a [successful strike against the smuggling of fake spirits](#). Shortly before Christmas 2019, Dutch customs authorities seized 47,000 bottles of counterfeit rum, an equivalent of 10 containers. The final destination of the seized bottles was Spain. OLAF investigators uncovered the modus operandi of the rum smugglers and located a suspicious warehouse in the Netherlands. OLAF also coordinated the action between the Dutch and Spanish customs authorities. The value of the counterfeit rum is estimated to be €2 million. (TW)

### Humanitarian Crisis in Syria: OLAF Detects Fraud and Misuse of EU Funds

On 24 March 2020, OLAF reported that it closed investigations in January 2020 that revealed [fraud by beneficiaries of a rule-of-law project in Syria](#). The EU had funded a UK-based company and its partner in the Netherlands and the United Arab Emirates with a total of nearly €2 million, in support of a project to deal with possible prosecutions for violations of international criminal and humanitarian law in Syria. OLAF investigators discovered that the claim to support the rule of law in Syria was false; in fact, the partners were committing widespread violations themselves, including

submission of false documents, irregular invoicing, and profiteering. OLAF recommended that the competent national authorities in the UK, the Netherlands, and Belgium recover almost the entire contractual sum and consider flagging the partners in the Commission's Early Detection and Exclusion System database.

On 7 February 2020, OLAF informed the public that it had closed an [investigation into the misuse of EU funds](#) provided to a well-known NGO for emergency assistance in Syria. The OLAF investigation detected a fraud and corruption scheme being carried out by two staff members of the NGO who siphoned taxpayers' money away from the humanitarian crisis in Syria and into their own pockets and those of their collaborators. OLAF also revealed significant shortcomings in the way in which the NGO had administered EU money. OLAF recommended the recovery of nearly €1.5 million from the NGO. (TW)

### OLAF Unveils Humanitarian Aid Fraud in Mauretania

In January 2020, OLAF [concluded investigations](#) against a Dutch company which revealed a fraud scheme against EU money for development and humanitarian aid as well as corruption. A Dutch company had won a large EU-funded contract managed by the Mauritanian authorities for the removal of 57 shipwrecks from a bay in Mauritania. OLAF and the Dutch authorities found that public procurement procedures had been breached, subcontract rules violated, and two Mauritanian officials bribed.

According to OLAF Director-General *Ville Itälä*, the case showed that OLAF also ensures the protection of EU money in non-EU countries, that OLAF fights for EU assistance to be received by those who need it, and that OLAF investigations know no borders. Detection of the fraud scheme was possible through on-the-spot checks, witness interviews, and analyses of large amounts of technical data. As a result of

the investigations, OLAF recommended the recovery of over €3 million and the prosecution of the fraudsters. In addition, OLAF recommended flagging the Dutch company in the Commission's Early Detection and Exclusion System (EDES), which would exclude the company from possible access to European taxpayers' money. (TW)

### European Public Prosecutor's Office

#### EPPO: Nomination of College Delayed, Budget Increase

The compilation of the College of the European Public Prosecutor's Office has been delayed. Due to the COVID-19 pandemic, the selection panel could not meet in March 2020; therefore, the appointment of recently nominated European Prosecutors had to be postponed. Initially, it was envisaged that the EPPO start its operational work in November 2020.

On 27 March 2020, the [European Commission proposed €3.3 million in additional funding](#) for the EPPO. The money is to be used for staff employment and IT equipment. In total, funding for the EPPO in 2020 has almost doubled (48%). By means of this increase in funding, the Commission has met the demands made by the European Chief Prosecutor, *Laura Kövesi*. The budget amendments have yet to be approved by the European Parliament and the Council. (TW)

### Europol

#### Stronger Collaboration with Mexico

In February 2020, Europol started negotiations for a collaboration with the Mexican Ministry of Security and Citizen Protection (SSPC) and the Mexican Ministry of Foreign Affairs. The aim is to sign a Working Agreement [to expand and intensify their collaboration](#) in preventing and combating serious crime such as the illicit flow of arms, arms

components, ammunition, and explosives.

To better support the EU Member States in preventing and combatting transnational organised crime, Europol's Management Board had recently included Mexico to the [list of priority partners](#) to conclude cooperation agreements with. (CR)

### EDPS Opinion on Europol Agreement with New Zealand Published

On 31 January 2020, the European Data Protection Supervisor (EDPS) published its [Opinion on the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and New Zealand](#). The Agreement shall provide the legal basis for the transfer of personal data between Europol and the New Zealand authorities that are responsible for fighting serious crime and terrorism. Their actions and mutual cooperation in preventing these crimes will be supported and strengthened.

In its opinion, the EDPS recommends, for instance, that the Agreement should explicitly lay down a list of criminal offences regulating which personal data can and cannot be exchanged. It should also include clear and detailed rules regarding the information that should be provided to the data subjects. Furthermore, it should specifically provide for periodic review of the need for storage of transferred personal data. The European Commission adopted a Recommendation for a Council Decision authorising the opening of negotiations for this agreement on 30 October 2019 (see also [eucrim 3/2019, p. 165](#)). (CR)

### Operation Against Counterfeit Medicine

At the beginning of March, [Operation 'Pangea'](#), a global operation targeted against trafficking in counterfeit medicines, resulted in the arrest of 121 persons and the dismantling of 31 organised criminal groups. The operation also indicated a significant increase in



the production of illicit pharmaceuticals and other medical products driven by the COVID-19 outbreak. As an example nearly 34,000 counterfeit surgical masks were seized and more than 2000 links related to bogus COVID-19 products were taken down. Operation ‘Pangea’ involved 90 countries worldwide, was coordinated by Interpol, and supported by Europol (CR)

### Hit Against Fuel Fraud

At the beginning of February 2020, law enforcement authorities from 23 EU Member States conducted a [major operation against Organised Crime Groups \(OCGs\) involved in fuel fraud](#). The operation led to 59 arrests, the seizure of 5.2 million litres of designer fuel worth approximately €6.8 million, and the seizure of €331,000 and other assets. It was led by the Hungarian National Tax and Customs Administration and the Slovak Financial Administration. Fuel fraud is a growing phenomenon used by OCGs to avoid excise duties. It typically involves base-oil fraud, also called designer fuel fraud, and fuel laundering. (CR)

### Staff Exchange

The second [staff exchange initiative](#) took place between the European Defence Agency (EDA), the permanent Computer Emergency Response Team (CERT-EU), the EU Cybersecurity Agency (ENISA), and Europol’s European Cybercrime Centre (EC3).

From 17 to 20 February 2020, experts from the different agencies met in Brussels to learn about each other’s priorities and practices, focusing on strategic developments in cyber defence. In addition, they met with industry representatives and were trained in threat hunting. (CR)

### Eurojust

#### Second Report on Encryption Published

In February 2020, Eurojust and Europol published their [second joint report on](#)

#### [the observatory function of encryption](#).

The report analyses the following:

- The progress of the encryption debate;
- The current legal landscape in which to address encryption in criminal investigations;
- Existing challenges.

The challenges include the following issues:

- Increasing use of encrypted communication devices by Organised Crime Groups (OCG);
- Policies and decisions by technology companies that influence the ability to access user data for the purpose of criminal investigations;
- The industry’s shift towards developments using End-to-End-Encryption (E2EE);
- The introduction of user-controlled encryption allowing users to have ultimate control over the encryption and decryption of their data;
- Homomorphic encryption allowing for data to be computed without compromising the privacy of that data;
- Information-hiding technologies, e.g., steganography;
- Quantum computing and 5G.

In its conclusions, the report pinpoints the overarching problem of conducting criminal investigations in contemporary society when sources of data by which to gather evidence are cut off. For the first joint report on encryption, see [eucrim 1/2019, p. 12](#). (CR)

#### Anti-Drug Trafficking Results 2019

In 2019, Eurojust and the EU Member States [tackled illicit drug trafficking worth over € 2.8 billion](#). Through action days, coordination meetings, and other judicial support, a total of 2686 suspects were able to be arrested or surrendered to other Member States. Approximately €2 billion in criminal assets were frozen and over a thousand weapons, mobile phones, laptops, and cars seized.

In numbers: Eurojust organised 27 coordination centres, 430 coordination meetings were held, and 800 agreements

made on the most effective strategies to prosecute suspects. The total number of cases increased from 3401 cases in 2014 to 7804 cases in 2019. 21,323 victims of crime were affected. (CR)

#### Action Against Large-Scale Bitcoin and Crypto-Currency Fraud

In January 2020, a Joint Investigation Team set up between authorities in Belgium and France and supported by Eurojust and Europol led to the arrest of ten suspects allegedly involved in an Organised Crime Group (OCG). The group had been [committing international fraud with the sale of bitcoins and other crypto-currencies](#).

Victims were contacted by phone and offered large profits on investments in bitcoins. Having made some initial gains, victims felt encouraged to make further investments, which the OCG then transferred to fake companies. The OCG later transferred the profits to bank accounts in various Asian countries and Turkey. The investigations unveiled further plans to commit fraud, which were not able to be realised. (CR)

### European Judicial Network (EJN)

#### Compilation on Judicial Cooperation under COVID-19 Available

The EJN is currently collecting and [compiling information](#) on the measures taken by the EU Member States in the area of international cooperation in criminal matters under the COVID-19 restrictions. The information is accessible for the EJN Contact Points under the [Restricted Area for Contact Points](#). (CR)

#### Updated Publication of European Criminal Law Texts Available

The compendium [“European Union instruments in the field of criminal law and related texts”](#) (see [eucrim 4/2019, p. 227](#)) is now available for download from the [EJN website](#). The publication contains a selection of 106 texts that are relevant in the field of European crimi-

nal law. Hard copies can be ordered from the Documentation Centre of the Council of the European Union. (CR)

## Frontex

### Cooperation with DG Migration and Home Affairs

On 5 February 2020, Frontex and the European Commission's Directorate-General for Migration and Home Affairs signed [Terms of Reference \(ToR\) to enhance their collaboration in the development of state-of-the-art technology for the border and coast guard community](#). Under the ToR, Frontex has been asked to identify research activities addressing capability gaps in the following areas: surveillance, situational awareness, biometrics, cybersecurity, and information availability and exchange. These gaps are to be translated into requirements for research solutions.

Furthermore, Frontex shall contribute to the development of solutions by facilitating their operational testing and validation within the framework of Frontex Joint Operations and in cooperation with national authorities. In order to better address national as well as its own operational needs, the Agency shall also monitor the outcomes of research and assess their operational relevance. Successful results shall be disseminated and exploited in order to facilitate their market uptake and use. Lastly, with the results and knowledge obtained from the Border Security research and innovation projects, Frontex will contribute to national capability development planning and the generation of the European Border and Coast Guard capability roadmaps. (CR)

### Rapid Border Intervention and the Greek-Turkish Border

On 2 March 2020, Frontex launched a [rapid border intervention](#) to assist Greece in dealing with the large numbers of migrants at its external borders to Turkey. Border guards and other relevant staff

as well as technical equipment will be deployed and provided by the Rapid Reaction and Rapid Reaction Equipment Pools. Consequently, [on 12 March 2020](#), 100 additional border guards from 22 EU Member States were deployed at the Greek land borders. Furthermore, Member States are providing technical equipment, including vessels, maritime surveillance aircraft, and Thermal-Vision Vehicles. Two additional Frontex border surveillance planes are in action. Prior to this rapid border intervention, Frontex already had more than 500 officers deployed in Greece, along with 11 vessels and various other equipment. (CR)

## Agency for Fundamental Rights (FRA)

### New FRA Website

Since February 2020, FRA has a [re-designed website](#) based on an enhanced, theme-based structure. Main themes include hate crime, asylum, and data protection. The new website highlights useful tools such as FRA's EU Fundamental Rights Information System (EFRIS) and provides country-specific information. It is also fully responsive across all mobile devices. (CR)

### Volume on FRA Published

A new book written by 24 human rights experts and published at the end of January 2020 looks at [FRA's impact during its 13-year existence](#). The book, entitled "Human Rights Law and Evidence-Based Policy – The impact of the EU Fundamental Rights Agency," reflects on FRA's experience throughout its first decade. It also examines the Agency's position in the policy environment, its role in researching applied rights, and its response to challenges and constraints. The book is available from [Routledge](#). (CR)

### FRA's Workplan in 2020

At the beginning of 2020, FRA published a [calendar with scheduled products for 2020](#). The calendar covers issues such as:

- Migration;
- Child rights;
- Disability;
- Roma;
- Ageing;
- Integration;
- Artificial intelligence, etc.

One of FRA's priorities for the year 2020 will be the national application of the EU's Fundamental Rights Charter.

Furthermore, the situation of Roma in different EU Member States will form a prominent part of FRA's work.

To complete its 2020 survey of lesbian, gay, trans, bisexual, and intersex people, FRA will take a closer look at the experiences of intersex people with the aim to further contribute to the European Commission's list of actions to advance the rights of LGBTI people across the EU. (CR)

## Specific Areas of Crime / Substantive Criminal Law

### Protection of Financial Interests

#### Budgetary Control Committee: EU Must Strengthen Fight Against Fraud

On 19 February 2020, the EP's Budgetary Control Committee (CONT) voted on the [discharge report](#) prepared by MEP [Monika Hohlmeier](#) (EPP, DE). By a 20 to 4 vote, the committee members [voted in favour of granting discharge](#) of the Commission's accounts for 2018 (corresponding to 97% of the entire EU budget). However, MEPs recommend a number of measures to fight fraud and avoid conflicts of interest:

- The Commission should introduce subsidy ceilings, so that EU financial support is distributed more fairly; it should be made impossible to receive subsidies amounting to hundreds of millions of Euros in one MFF-period;
- The Commission should create rules that allow disclosure of the end beneficiaries of agricultural funds;
- The EU must establish a complaint

mechanism enabling farmers to inform the Commission of organised crime or other malpractices (e.g., land-grabbing, forced labour, etc.);

- Future guidelines must tackle conflicts of interest with regard to high-profile politicians;

- The newly created European Public Prosecutor's Office is underfinanced and not fully operational in conjunction with current budget planning; based on an estimated caseload of 3000 cases per year, the EPPO needs at least 76 additional posts and €8 million in funding;

- MEPs insist on the adoption of the regulation enabling the EU to restrict EU money for rule-of-law violations in a Member State (this regulation is [currently blocked in the Council](#)).

The CONT report comes in preparation for the [EP's discharge decision](#). The discharge is one of the most important rights of the EP.

## Money Laundering

### EBA Report on Performance of AML/CFT Banking Supervision

**spot light** Authorities still face challenges in the AML/CFT supervision of banks. Measures to correct deficiencies in banks' anti-money laundering and countering the financing of terrorism (AML/CFT) systems and controls should be more dissuasive. These are one of the main conclusions of the European Banking Authority's (EBA) [first report on competent authorities' approaches to the AML/CFT supervision of banks](#). It is part of the EBA's new duties to ensure consistent and effective application of the EU's AML/CFT law.

The report is based on a peer review of seven supervisory authorities in five EU Member States that was carried out in 2019. It describes how these competent authorities apply the risk-based approach according to international standards, Directive (EU) 2015/849 (the 4th AMLD), and the European Supervisory Authorities' joint AML/CFT guidelines.

The EBA report acknowledges that all authorities in the sample have taken significant steps to strengthen their approach to AML/CFT supervision. Supervisory staff is well-trained and committed to fighting financial crime. Several authorities have also made the fight against ML/TF one of their key priorities and significantly expanded their AML/CFT supervisory teams in a number of cases. The report also observes, however, that most authorities faced challenges in operationalising the risk-based approach to AML/CFT. A number of challenges are common to all peer-reviewed authorities and may therefore hold true for other supervisory authorities in all EU Member States. The major challenges are as follows:

- Translating theoretical knowledge of ML/TF risks into supervisory practice and risk-based supervisory strategies;

- Moving away from a focus on tick box compliance towards assessing the effectiveness of banks' AML/CFT systems and controls;

- Taking sufficiently dissuasive corrective measures if banks' AML/CFT control systems are not effective;

- Cooperating effectively with domestic and international stakeholders to draw on synergies

- Positioning AML/CFT in the wider national and international supervisory frameworks.

These challenges can result in ineffective banking supervision. The EBA's peer review will be continued in 2020. The EBA will also continue to provide support and training to all competent EU AML/CFT authorities in order to help them tackle the key challenges identified in the present report. The EBA is also working on a review of its AML/CFT guidelines in order to provide further guidance in areas where weaknesses persist. It has launched a [public consultation](#) on the revised draft guidelines. Stakeholders are invited to comment by 6 July 2020.

The EBA has also published a [factsheet](#) explaining its new functions

in coordinating, leading, and monitoring the fight against money laundering and terrorist financing in more detail. (TW)

### Commission Roadmap on Future AML/CFT Actions

On 12 February 2020, the Commission published the [roadmap "towards a new comprehensive approach to preventing and combating money laundering and terrorism financing."](#) The roadmap launched a public consultation on possible ways to overhaul current EU AML/CFT legislation. It follows the AML package presented by the Commission in July 2019 ([see eucrim 2/2018, pp. 94–97](#)). In this package, the Commission highlighted a number of deficiencies in implementation of the EU anti-money laundering framework and the need to develop a new comprehensive approach at the EU level. The debate is fuelled by recent money laundering scandals, which, according to the Commission, show the full implementation of the most recent provisions introduced by the 5th AML Directive. The 2018 Council AML/CFT action plan cannot remedy the current weaknesses.

The Commission's initiative now aims at sounding out the areas in which further action is needed at the EU level in order to achieve a comprehensive and effective framework to prevent criminals from laundering the proceeds of their illicit activities and to prevent the financing of terrorism. It prepares further work which might result in concrete legislative proposals.

The Commission will also respond to demands from the EP to carry out a more fundamental reform of the current EU AML/CFT legal framework, in particular replacing the current AML directives with a directly applicable EU regulation. In light of the recent Luanda Leaks, MEPs reiterated their position when they discussed the [state of play of the EU fight against money laundering in the plenary session](#) on 12 February 2020. (TW)

### Infringement Procedures for Non-Transposition of 5th AML Directive

On 12 February 2020, the Commission [started infringement proceedings against eight Member States](#) for not having transposed the 5th Anti-Money Laundering Directive ([Directive \(EU\) 2018/843](#); see also [eucrim 2/2018, pp. 93–94](#)). The Commission sent [letters of formal notice](#) to Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia, and Spain, because the countries have not notified any implementation measure for the 5th AML Directive. The Commission stressed the importance of the Directive's rules for the EU's collective interest. EU Member States were to have transposed the Directive by 10 January 2020. The Member States concerned now have two months to deliver a satisfying response; otherwise, the Commission will send them reasoned opinions. (TW)

### Tax Evasion

#### New Legislation to Fight VAT Fraud in Cross-Border E-Commerce

In February 2020, the Council [adopted new legislative measures to combat cross-border VAT fraud](#) caused by the fraudulent behaviour of some businesses in the area of cross-border e-commerce. The reform will introduce obligations for payment service providers, e.g., banks, to keep sufficiently detailed records and to report certain cross-border payments, thus enabling the location of the payer and the payee to be more easily identified. It will help facilitate controls of the supplies of goods and services by the competent Member State authorities.

In addition, a new central electronic system of payment information ("CESOP") will be set up for storage of the payment information and for further processing of this information by national anti-fraud officials. CESOP will store, aggregate, and analyse all VAT-relevant information regarding payments trans-

mitted by Member States in relation to individual payees. CESOP will enable a full overview of payments received by payees from payers located in the Member States and make the results of specific analyses of information available to Eurofisc liaison officials. The data in CESOP can also be cross-checked with other European databases.

The new rules shall apply from 1 January 2024. They consist of two legal acts amending existing EU legislation in the field of VAT:

- Council [Regulation \(EU\) 2020/283](#) of 18 February 2020 amending Regulation (EU) No 904/2010 as regards measures to strengthen administrative cooperation in order to combat VAT fraud (*O.J. L 62, 2.3.2020, 1*);
- Council [Directive \(EU\) 2020/284](#) of 18 February 2020 amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers (*O.J. L 62, 2.3.2020, 7*).

Against the background of this new legislation, on 18 March 2020, the European Commission published a [survey for actors in the payment industry](#). The survey aims to gather input from the different actors in the payment industry regarding the new reporting obligations introduced by Directive (EU) 2020/284. It gathers their views on implementation of the legislative package on the transmission and exchange of payment data in order to fight VAT fraud. The results will feed the work of the expert group established to implement the new VAT regulations. (TW)

#### Kiel Study: EU's Trade Self-Surplus Goes Back to VAT Fraud

In a [working paper](#) published in January 2020, the Kiel Institute for the World Economy (IfW) and the ifo Institute in Munich, Germany elucidate that the main reason for the EU's large trade surplus with itself is apparently large-scale VAT fraud. By applying forensic accounting methods, the researchers observed that the EU runs a trade surplus with itself of €307 billion or 1.9 percent

of the Union's GDP in 2018. The working paper analysed data over a large period of time. Apparently, the EU's trade self-surplus has become persistent over time: the EU has had a self-surplus since 1993, when the single market was established. This surplus has increased considerably with the 2004 enlargement of the EU and grown to a total of €2.9 trillion over the past twelve years.

The researchers argue that the figure should be zero if all transactions were properly reported and recorded. The phenomenon cannot be explained by measurement errors or incidental inaccuracies only, but rather the large fraction of the EU's self-surplus seems to be related to fraud in value added tax. It is estimated that EU-wide VAT revenue shortfalls could range from €27 to 35 billion per year in a realistic scenario. At worst, revenue shortfalls would even amount to €64 billion.

The researchers also point out that data quality varies among the Member States. The differences were most pronounced between EU neighbouring countries and also between Member States with the more divergent VAT rates. As a result of the study, the following recommendations were made:

- Institutions in charge should substantially improve the quality and reliability of intra-EU data on the balance of payment;
- An electronic clearing procedure should be established to make tax fraud and data misreporting very difficult;
- The non-disclosure or non-collection of certain balance-of-payment items (e.g., primary income) should be dealt with urgently.

The study shows that tackling VAT fraud in the EU should be a top priority, because the large trade self-surplus is fuelling international disputes. (TW)

#### Commission Announces New Initiatives to Tackle Tax Evasion

The European Commission announced that it will adopt a [new action plan to fight tax evasion](#) in the second quarter of



2020. The Commission opened a public consultation for this purpose. The Action Plan will not only include key initiatives to tackle tax evasion and tax fraud but also to simplify the tax system in order to make compliance easier. It will also launch the External Strategy on tax good governance 2020.

The Commission points out that billions of euros are lost due to tax evasion every year in the EU (see also the news item on the recent Kiel study on VAT fraud). On the one hand, efforts by national tax authorities to tackle tax evasion are increasingly being hampered by new business models, especially those based on digital technology. On the other hand, companies that do business in the single market need a simpler and more up-to-date tax system.

Against this background, the new Action Plan is to implement *Ursula von der Leyen's* vision that Europe will be “an economy that works for people.” This includes fair taxation, so that everybody pays their fair share, and the creation of a tax environment in which the economy can grow. The Action Plan is also to take advantage of the latest developments in technology and digitalisation. (TW)

### Council Revises List of Non-Cooperative Tax Jurisdictions

On 18 February 2020, the Economic and Financial Affairs Council revised the [EU list of non-cooperative jurisdictions for tax](#) purposes. By blacklisting certain countries, the EU aims to promote good tax governance at the global level. The list includes jurisdictions that either have not engaged in a constructive dialogue with the EU on tax governance or failed to deliver on their commitments to implement reforms complying with the EU's criteria on time.

Next to the eight countries already on the [blacklist](#) (American Samoa, Fiji, Guam, Oman, Samoa, Trinidad and Tobago, US Virgin Islands, Vanuatu), the Council added Palau, Panama, Seychelles, and – as the first British Overseas Territory – Cayman Islands. Other

British Overseas Territories (Bahamas, Bermudas, and British Virgin Islands) were removed from the list, as the Council considered these jurisdictions to be in line with the international tax standards in the meantime. This move was criticised by tax transparency organisations. The Council also removed 13 additional jurisdictions from the “black list.”

Thirteen countries remain on a “grey list” (including, e.g., Turkey, Bosnia-Herzegovina, Morocco, and Australia). This list (Annex II of the Council conclusions) covers jurisdictions that showed cooperation and are set to deliver on their reform commitment, although they have not yet met the international tax standards. The Council partly granted deadline extensions to these countries.

The Council will continue to regularly review and update the list in the coming years, taking into consideration the evolving deadlines for jurisdictions to deliver on their commitments and the development of the listing criteria that the EU uses to establish the list. (TW)

### Tax Policies in the European Union – 2020 Survey

On 31 January 2020, the European Commission (DG TAXUD) published the fourth edition of its [survey on “tax policies in the EU.”](#) The survey examines how Member States' tax systems perform in respect of the following benchmarks:

- Stimulating investment and addressing positive and negative externalities;
- Improving tax administration and tax certainty;
- Developing a more employment-friendly environment;
- Correcting inequalities and promoting social mobility;
- Fighting tax fraud, evasion, and avoidance.

These benchmarks in mind, the report identifies possible improvements to tax systems in terms of tax design, implementation, and compliance.

After defining what makes a fair and efficient tax system and providing an

overview of recent taxation trends, the survey outlines how national taxation systems perform against the five benchmarks. The aim is to help Member States find the best way to address their own specific tax challenges. The survey then reviews Member States' most recent tax reforms and describes some general reform options. Lastly, it presents the major recent actions on tax matters at EU level (2014–2020). New elements of the present edition of the survey include, inter alia, discussions on:

- Tax competition;
- Design and distribution of the overall tax mix;
- Sustainability of tax systems in a changing world;
- Measurement of effective tax rates on corporate income.

The survey provides evidence that multinational enterprises continue to engage in aggressive tax planning in order to decrease their tax burden. In addition, billions of euros in tax revenue are lost in the EU each year, because individuals evade taxes. According to the survey, taxation is more than just about raising revenue but also plays a central role in shaping a fairer society. Right and fair tax policies can eventually contribute to achieving the goals of the European Green Deal.

One of the main conclusions is that there is scope for Member States' tax systems to be fairer and more efficient. This can be accomplished by various means, including tax incentives, reduced tax burdens on low-income earners, tax policies to foster social mobility, and the creation of effective tools to fight tax avoidance. The Commission admits, however, that there is no “one size does fit all” rule, but instead tax policies must take account of the national specificities and circumstances.

The survey on tax policies in the EU is an important tool in the context of the [European Semester](#) and substantiates the tax policy priorities of the Commission's [Annual Sustainable Growth Strategy](#). (TW)

## Evaluation of the Tobacco Taxation Directive

On 10 February 2020, the European Commission published the results of its evaluation of [Directive 2011/64/EU](#), which provides for the structure and rates of excise duties on manufactured tobacco (i.e., cigarettes, cigars and cigarillos, fine-cut tobacco for rolling cigarettes, and other smoking tobacco). The Directive identifies which tobacco products are subject to the harmonised rules for excise duties and sets minimum levels of taxation. It aims at ensuring the proper functioning of the internal market, at a high level of health protection, and at bolstering the fight against tax fraud, tax evasion, and illegal cross-border shopping.

The [evaluation assesses](#) to which extent implementation of the Directive's provisions has contributed to achieving the objectives. In line with the EU's [Border Regulation Guidelines](#), it was carried out according to the basic evaluation criteria of effectiveness, efficiency, relevance, coherence, and EU added value. The main findings are as follows:

- The current legislation has been working well in terms of the predictability and stability of fiscal revenues for Member States;
- The Directive allows Member States enough flexibility to implement their national fiscal policies for traditional tobacco products (with €82.3 billion excise tax revenue in the EU in 2017);
- New products, such as e-cigarettes or heated tobacco products, illustrate the limits of the current legal framework, which is unable to cope with these increasingly developing markets;
- The impact of the tobacco taxation Directive on public health has been moderate;
- Significant differences in taxes (hence prices) between Member States also limit the objective of achieving public health, particularly where there is a high level of cross-border shopping;
- Although illicit trade in cigarettes and fine-cut tobacco have decreased

slightly over the years, this area remains a substantial challenge. It is estimated that the EU potentially loses €7.5 billion in excise revenues, which calls for strengthening enforcement policies and designing tax regimes with enforcement safeguard measures;

- There has been an increase in the illicit manufacturing of cigarettes within the EU, requiring a harmonised approach to monitoring the flow of raw tobacco within and into the EU.

Ultimately, the evaluation report calls for a more comprehensive and holistic approach, because Directive 2011/64 is not much coherent with other EU policies. This approach should take into account all aspects of tobacco control, including public health, taxation, the fight against illicit trade, and environmental concerns. (TW)

## Organised Crime

### Impact of COVID-19 on Serious and Organised Crime

**spot light** On 27 March 2020, Europol published a [report on exploitation of the COVID-19 pandemic by criminals](#). The report, which aims to support EU Member States' law enforcement, looks at the impact of measures taken by governments against the COVID-19 crisis on serious and organised crime. The report analyses the impact of the crisis in four key areas: cybercrime, fraud, trafficking in counterfeit and substandard goods, and organised property crime. Furthermore, it takes a brief look at other criminal activities.

In the area of cybercrime, the report sees a further increase in the number of cyberattacks involving various malware and ransomware packages themed around the COVID-19 pandemic. The threat of cyberattacks against critical health infrastructure is seen as a major risk.

According to the report, a large number of new or adapted fraud and scam schemes is expected to emerge. It seems

that investment are being adapted to elicit speculative investments in stocks related to COVID-19. One special form involves supply scams attacking businesses providing supplies to prevent COVID-19, e.g., protective masks. With regard to counterfeit and substandard goods, the report notes a booming market in the pandemic economy, especially with regard to medical products.

As far as organised property crime is concerned, the report finds criminals' *modi operandi* being adapted to already existing schemes involving theft, e.g., the impersonation of relatives or authorities (faking and entering) in 'Corona' situations.

Lastly, looking at other criminal activities, the report finds it difficult to assess the short-term impact of the COVID-19 crisis on the drug trafficking market, but anticipates that supply shortages will translate into increased drug-related violence between rival suppliers and distributors.

The demand for migrant smuggling services may increase, with new movements being undertaken to circumvent the enhanced border control measures. Sexual exploitation may increase due to the closure of establishments offering legal sex work.

The report is based on information received by the EU Member States on a 24/7 basis. (CR)

## Cybercrime

### EU's 5G Cybersecurity Toolbox

On 29 January 2020, the Commission tabled an [EU toolbox of mitigating measures](#) with the consensus of EU Member States in order to address security risks related to the rollout of 5G, the fifth generation of mobile networks. Ensuring protection of 5G from cybersecurity threats is one of the EU's top strategic priorities. The concrete proposals in the toolbox follow the [European Council conclusions](#), which called for a concerted approach to the 5G security,

as well as the ensuing [Commission Recommendation](#) for Member States to take concrete actions to assess cybersecurity risks of 5G networks and to strengthen risk mitigation measures (both adopted/issued in March 2019).

The toolbox lays out a range of security measures, allowing the effective mitigation of risks and ensuring that secure 5G networks are deployed across Europe. It sets out detailed mitigation plans for each of the identified risks and recommends a set of key strategic and technical measures to be taken by all Member States and/or by the Commission. Member States should take first concrete, measurable steps to implement the key measures by 30 April 2020 (see also the Commission Communication “Secure 5G deployment in the EU – Implementing the EU toolbox,” [COM\(2020\) 50 final](#)). They are also invited to prepare a joint report on implementation in each Member State by 30 June 2020. By October 2020, the Commission plans a review of its March 2019 Recommendation. (TW)

### Eurobarometer: Europeans Attitudes Towards Cyber Security

Alongside the presentation of the EU toolbox on joint security measures for 5G networks in January 2020, a [special Eurobarometer survey](#) was published that aimed at identifying EU citizens’ awareness, experience, and perception of cyber security. The fieldwork was carried out in October 2019. The main findings of the survey are as follows:

- The majority of respondents (52%) feel that they are not able to protect themselves sufficiently against cybercrime (while the figure was much higher (71%) in 2017);
- Awareness of cybercrime is rising, with 52% of respondents stating that they are fairly well or very well informed about cybercrime (up from 46% in 2017);
- Bank card or online banking fraud, infection of devices with malicious software, and identity theft were reported

as the most frequent concerns about becoming a victim of cybercrime;

- A large majority (77%) are unaware of the means to report a crime;
- A large majority (70%) did not report a cybercrime.

The survey also informs on the percentage which measures are taken by the internet users in reaction of cybercrime threats. (TW)

### Cyber Information and Intelligence Sharing Initiative Launched

Europol launched the “Cyber Information and Intelligence Sharing Initiative (CIISI-EU)” together with the European Central Bank and a group of Europe’s largest and most important financial infrastructures. The aim is to protect the European financial system from cyber-attacks.

The initiative of 27 February 2020 brings together central banks, clearing houses, stock exchanges, and payment system providers as well as Europol and the European Union Agency for Cybersecurity (ENISA) in order to share vital cybersecurity threat information. Key issues concern:

- The ability to understand the threat;
- The ability to provide for a collective response;
- Awareness raising concerning protective measures needed to achieve a change in behaviour amongst financial institutions. (CR)

### Racism and Xenophobia

#### Terrorist Content Online Regulation – Controversies in Trilogue

On 21 January 2020, the LIBE Committee discussed the Commission proposal for a regulation on preventing the dissemination of terrorist content online (for the proposal, see [eucrim 2/2018, 97–98](#) and the article by *G. Robinson*, [eucrim 4/2018, p. 234](#)). Rapporteur *Patryk Jaki* (ECR, PL) outlined that agreements with the trilogue partners were reached on broad parts of the proposal.

The Commission still has reservations, however, insisting that cross-border removal orders be directly enforced by hosting service providers and voicing concern over the deployment of automated detection tools. By contrast, MEPs stressed that the freedom of expression must also be safeguarded in the Internet; they are against the obligation to use ex-ante control measures or “upload filters” (see also the [report on the proposal](#) by LIBE member *Daniel Dalton* of 9 April 2019; see also in this context the EP resolution of 17 April 2019 and [eucrim 1/2019, p. 21](#)). Civil stakeholders identified additional critical issues and oppose the EU’s approach (see [eucrim 1/2019, p. 22](#)). In his [formal comments](#) of February 2019, the European Data Protection Supervisor encouraged the EU legislator to respect fundamental rights, in particular data protection, and to take into account the principles of quality of law and economic certainty (see details at [eucrim 1/2019, p. 21](#)). (TW)

## Procedural Criminal Law

### Procedural Safeguards

#### CJEU: Prosecutor Can Balance Defence Rights Against Effective Fraud Prosecution (Kolev II)

In [Case C-612/15](#) (criminal proceedings against *Nikoley Kolev*, *Stefan Kostadinov*, judgment of 5 June 2018, see [eucrim 2/2018, pp. 99/101](#)), the CJEU ruled that Union law, i.e., the obligation to protect the EU’s financial interests in accordance with Art. 325(1) TFEU, precludes national legislation that establishes a procedure for the termination of criminal proceedings, such as that provided for in Arts. 368 and 369 of the Bulgarian Code of Criminal Procedure, in so far as that legislation is applicable in proceedings initiated with respect to cases of serious fraud or other serious illegal activities affecting the financial interests of the European Union in cus-

toms matters. The CJEU added that it is up to the national court to give full effect to Art. 325(1) TFEU by disapplying that legislation, where necessary, while also ensuring respect for the fundamental rights of the persons accused.

Following this judgment, the referring court wished to remedy itself the procedural irregularities that had occurred during the pre-trial phase of the criminal proceedings against the defendants. The irregularities concerned their right to be informed about the charges and to access the case material, although the trial phase had already been terminated and the case referred back to the prosecutor. The appeal court criticised this action on the part of the referring court, because it was contradictory to national procedural law. The appeal court requested that the referring court refer the case back to the prosecutor.

The referring court again referred the case to the CJEU, seeking clarification on whether Union law precludes the interpretation made by the appeal court (*Case C-704/18, Kolev II*). The referring court argued that the injunction of the appeal court would make it impossible to comply with the operative part of the CJEU judgment according to which the defendants' rights in Arts. 6 and 7 of Directive 2012/13 must be implemented.

In its *judgment of 12 February 2020*, the CJEU clarified that the choice on how the defendants' rights are ensured falls within the procedural autonomy of the Member States. In applying the principles of equivalence and effectiveness, the CJEU concludes that, as it is with the criminal court, the prosecutor is also able to guarantee the rights of the defence in the pre-trial phase. Hence, there is nothing wrong with the injunction of the higher court (imposed on the referring court to refer the case back to the prosecutor), after termination of the trial phase of the criminal proceedings, for procedural irregularities committed during the pre-trial phase of those proceedings to be remedied. (TW)

### CJEU: Accused Person Can Waive Right to Be Present at Trial

The CJEU ruled on the conditions under which the non-appearance of accused persons at certain trial hearings for reasons either within or beyond their control is compatible with Union law. The concrete case deals with the provisions of the Bulgarian Criminal Code of Procedure on "trials in absentia" and which was brought to the CJEU by the Spetsializiran nakazatelen sad (Special Court for Criminal Cases, Bulgaria): the CJEU interpreted the right to be present at trial guaranteed by Art. 8 of Directive 2016/343 (for the Directive, see *eucri* 1/2016, p. 13 and the article by *S. Cras/A. Erbežnik, eucri* 1/2016, pp. 25–36). In its judgment of 13 February 2020 (*Case C-688/18, criminal proceedings against TX and UW*), the CJEU did not object to the Bulgarian rules.

The CJEU refers to recital 35 of Directive 2016/343, which states that the right of suspects and accused persons to be present at the trial is not absolute. In fact, under certain conditions, suspects and accused person should be able to, expressly or tacitly, but unequivocally, waive that right. The judges in Luxembourg took up the case law of the ECtHR, according to which such waiver of the right to take part in the hearing must be established unequivocally and be attended by minimum safeguards commensurate with its seriousness. Furthermore, it must not run counter to any important public interest.

In situations where the accused did not appear in hearings for reasons which are beyond his control, a waiver must be flanked with guarantees that procedural steps, which were taken during his non-appearance (e.g., questioning of a witness), can be repeated. This is the case under Bulgarian law.

The CJEU stressed, however, that Directive 2016/343 lays down only common minimum rules applicable to criminal proceedings concerning certain aspects of the presumption of innocence

and the right to be present at the trial. In light of the minimal degree of harmonisation, the Directive therefore cannot be understood as a complete and exhaustive instrument. (TW)

### German Bar Association Calls for Further Strengthening of Procedural Safeguards in EU

The German Bar Association (Deutscher Anwalt Verein – DAV) called on the establishment of additional minimum guarantees for procedural rights within the EU. In its *statement No 5/20 of January 2020*, the association assesses the state of play of procedural safeguards in the EU on the basis of the six Directives implemented since the 2009 Roadmap. According to the statement, without effective control mechanisms to implement these directives, the introduction of new instruments will only lead to limited improvement in procedural rights in the EU. The right to access case materials, enshrined in Art. 7 of Directive 2012/13, for instance, requires further concretisation. Given that the existing directives only cover part of the (minimum) harmonisation, the German Bar Association advocates new initiatives. In this context, the statement expressly welcomes the proposals for a new Roadmap 2020 by the ECBA (see *Matt*, guest editorial, *eucri* 1/2017, p. 1). Among the measures proposed, the German Bar Association considers the following three areas important for new EU initiatives:

- Minimum standards for pre-trial detention;
- Conflicts of jurisdiction and ne bis in idem;
- Admissibility and exclusion of evidence.

The German Bar Association also calls for revision of the Framework Decision on the European Arrest Warrant, ideally to take into account the CJEU's case law in this area, correct the existing deficits, and introduce effective remedies against the issuance of a EAW in the issuing State. (TW)



## Data Protection

### AG: Data Retention Should Be Strictly Limited

**spot light** Advocate General (AG) *Manuel Campos Sánchez-Bordona* advocates that the CJEU's rather restrictive case law on the retention of personal data and access to these data by law enforcement or intelligence authorities should be upheld. Following the judgment in the Joined Cases C-203/15, *Tele2 Sverige*, and C-698/15, *Tom Watson and Others* (see [eucrim 4/2016, p. 164](#)), the CJEU now has to deal with further references for preliminary rulings. The AG's opinion is linked to references initiated by national courts in France, Belgium, and the UK. All seek clarification as to whether their national legislation on data retention is in line with EU law. The courts criticised the CJEU for having established hurdles that are too high; the requirements set out in *Tele2 Sverige/Watson* deprive the EU Member States of an instrument that is absolutely necessary in order to combat terrorism and safeguard national security, thus putting corresponding national security measures at risk. The references are as follows:

- **Case C-623/17:** Request for a preliminary ruling from the Investigatory Powers Tribunal (UK) in the case *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*. The main proceedings at the referring court concern the acquisition and use of bulk communications data by the United Kingdom Security and Intelligence Agencies (SIAs) via the operators of public electronic communications networks for the purpose of protecting national security, e.g., in the fields of counter-terrorism, counter-espionage, and counter-nuclear proliferation.

- **Joined Cases C-511/18 and 512/18:** both requests for a preliminary ruling

came from the Conseil d'État (France) in the cases *La Quadrature du Net*, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées. The Conseil d'État essentially seeks clarification as to whether two obligations imposed on telecommunication service providers under French legislation are compatible with EU law: i.e., a) the (real-time) collection of specific data; b) the retention of location and traffic data in order to facilitate identification of any person who is civilly and criminally liable.

- **Case C-520/18:** Request for a preliminary ruling from the Cour constitutionnelle (Belgium) in the case: *Ordre des barreaux francophones et germanophones, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres*. The Belgian court wonders whether the Belgian rules on the retention of data which follow multiple objectives (e.g., including the investigation, detection and prosecution of offences other than serious crime and the attainment of the defence of the territory and of public security) are compatible with EU law. In addition, the referring court asks whether it might maintain the effects of the national law on a temporary basis if a failure with EU law is concluded.

Although the AG issued three separate opinions, he clarifies that all cases before the CJEU [raise common problems](#). In essence, the yardstick for all cases is [Directive 2002/58/EC](#) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the fundamental rights enshrined in the CFR.

First, the AG examines the applicability of Directive 2002/58/EC. Although Art. 1 para. 3 of the Directive excludes from its scope “activities concerning public security, defence,

State security (...) and the activities of the State in areas of criminal law,” the AG concludes that this exemption only refers to specific activities by the State authorities on their own account. In data retention situations, however, obligations are imposed on private parties, whose cooperation is required. Even if this cooperation is required for national security interests, these activities are governed by the Directive, i.e., the protection of privacy, which is enforceable against private actors. Accordingly, Directive 2002/58 is applicable in the data retention scenarios.

Second, the AG deals with the possibility under Art. 15 para. 1 of Directive 2002/58. Under certain conditions, it allows Member States to adopt legislative measures providing for the retention of data if these measures follow objectives of safeguarding national security, defence, public security, and the prevention, investigation, detection, and prosecution of criminal offences or of unauthorised use of the electronic communication system. Limitations to the privacy rights enshrined in the Directive (in particular, the guarantee of confidentiality of communications and related traffic data) must be interpreted strictly and with regard to the fundamental rights enshrined in the CFR. The AG proposes upholding the case law of the judgment *Tele2 Sverige /Watson*. From the Union law perspective, it is disproportionate and unlawful if national laws establish a general and indiscriminate retention of all traffic and location data of all subscribers and registered users. By contrast, a Member State can follow the approach of limited and discriminate retention flanked with limited access to said data. This would entail the following aspects:

- Retention of specific categories of data that are absolutely essential for the effective prevention and control of crime and the safeguarding of national security;

- Retention for a determinate period adapted to each particular category;

- Data access subject to a prior review carried out either by a court or by an independent administrative authority;
- Notification of data subjects (provided that ongoing investigations are not jeopardised);
- Adoption of rules to avoid misuse of, and unlawful access to, retained data.

The AG stressed, however, that it is not the task of the CJEU to develop a lawful data retention model. This must be done by the legislator.

Further developing the previous case law, the AG suggests that imposing a more extensive and general data retention regime is possible for “exceptional situations characterised by an imminent threat or an extraordinary risk warranting the official declaration of a state of emergency.” However, such a regime can also only be lawful for a limited period and it must be proportionate.

As regards the concrete cases at issue, the AG concludes that Union law precludes the established national data retention legislations in France, Belgium, and the UK, because they are general and indiscriminate. There is, however, no preclusion for the specific part of French law that permits the real-time collection of traffic and location data of individuals, “provided that those activities are carried out in accordance with established procedures for accessing legitimately retained personal data and are subject to the same safeguards.”

As regards the specific question posed by the Belgian court, the AG proposes that “a national court may, if its domestic law so permits, maintain the effects of legislation such as the Belgian legislation, on an exceptional and temporary basis, even where that legislation is incompatible with EU law, if maintaining those effects is justified by overriding considerations relating to threats to public security or national security that cannot be addressed by other means or other alternatives, but only for as long as is strictly necessary to correct the incompatibility with EU law.”

If the CJEU follows the opinion of

AG *Campos Sánchez-Bordona*, the cases at issue may have an impact on other jurisdictions. This includes the request for a preliminary ruling by the Federal Administrative Court of Germany asking for verification of the lawfulness of the 2015 German law on data retention (see [eucrim 3/2019, p. 176](#)). On 21 January 2020, AG *Pitruzzella* also published his opinion on interpretation of the Estonian data retention legislation (see separate news item). (TW)

### AG: Conditions of Access to Retained Telecommunications Data for Law Enforcement

Advocate General *Giovanni Pitruzzella* presented his opinion on the Estonian data retention law, advising on how Member States may arrange the contentious retention of personal data for law enforcement purposes while keeping in line with Union law ([opinion of 21 January 2020, Case C-746/18, H.K. v Prokuratuur](#)).

The case is related to criminal proceedings against H.K. for several robberies, fraud, and violence against parties to court proceedings. The criminal court of first instance based H.K.’s conviction on, *inter alia*, reports drawn up using data relating to electronic communications in accordance with the established Estonian data retention law. The investigating authority had obtained the data from a telecommunications service provider in the pre-trial procedure, after having been granted authorisation from an assistant public prosecutor. The data provided insight into the location, length, partners, etc. of the accused’s communication within a given period of time. H.K. argued that the reports are inadmissible evidence and his conviction therefore unfounded.

The Estonian Supreme Court, indeed, had doubts on the compatibility with EU law of the circumstances in which investigating authorities had access to that information. The Estonian Supreme Court raised the question of whether Art. 15(1) of [Directive 2002/58/EC](#) on privacy and

electronic communications, read in the light of Arts. 7, 8, 11, and 52(1) CFR, must be interpreted as meaning that the categories of data concerned and the duration of the period for which access is sought are among the criteria for assessing the seriousness of the interference with fundamental rights that is associated with the access by competent national authorities to the personal data that providers of electronic communications services are obliged to retain under national legislation.

AG *Pitruzzella* confirmed this view. Examining the lessons learned from the judgments in *Tele2 Sverige/Watson* (Joined Cases C-203/15 and C-698/15, see [eucrim 4/2016, p. 164](#)) and *Ministerio Fiscal* (Case C-207/16, see [eucrim 3/2018, pp. 155–157](#)), the AG concludes that both the categories of data concerned and the duration of the period for which access to these data is sought are relevant. He further states that, depending on the seriousness of the interference, it was up to the referring court to assess whether this access was strictly necessary to achieve the objective of preventing, investigating, detecting, and prosecuting criminal offences.

In addition, the Estonian Supreme Court posed the question of whether the public prosecutor who granted access – also in view of the various duties assigned to it under Estonian law – can be considered an “independent” administrative authority. This question refers to the CJEU requirement set out in its *Tele2 Sverige/Watson* judgment in that access to retained data “should, as a general rule, ... be subject to a prior review carried out *either by a court or by an independent administrative body*, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime.” The AG maintains that this requirement is not met by the public prosecutor’s office, because it is responsible for directing the pre-trial procedure, on

the one hand, while also being likely to represent the public prosecution in judicial proceedings, on the other.

The AG's opinion on the Estonian data retention law comes shortly after the opinion of his colleague *Manuel Campos Sánchez-Bordona*, who examined the general lawfulness of data retention regimes in France, Belgium, and the UK. The topic of data retention will continue to keep the CJEU busy. (TW)

### Council Endorses Start of Negotiations on EU-Japan PNR Deal

On 18 February 2020, the [Council gave green light to the Commission](#) to start negotiations with Japan on an agreement on the transfer and use of passenger name record (PNR) data. The Council endorsed the respective negotiating directives recommended by the Commission in September 2019 (see [eucrim 3/2019, p. 175](#)). The Agreement will set out the framework and conditions for the exchange of PNR data, so that they can be used to prevent and fight terrorism and serious crime. PNR data is personal information provided by passengers, which is collected and held by air carriers (e.g., name of passenger, travel dates, itineraries, seats, baggage, contact details, and means of payment).

The data transfer to Japan will be in line with the EU General Data Protection Regulation as the [Commission attested Japan](#) to guarantee an adequate level of protection of personal data in January 2019. (TW)

### Commission Presents European Data Strategy

On 19 February 2020, the Commission unveiled its plans and actions for a [European data strategy](#). The new Commission under President *Ursula von der Leyen* set the ambitious goal that the EU become the leading role model for a society empowered by data to make better decisions – in business and in the public sector. All European citizens and businesses should benefit from new technologies and the use of data. The

digital-agile economy must be boosted. The European Data Strategy aims at creating a single market for data with the following features:

- Data flow within the EU and across sectors, for the benefit of all;
- Full respect for European rules, in particular on privacy and data protection as well as on competition law;
- Fair, practical, and clear rules for access and use of data.

In its [Communication](#) on a European data strategy, the Commission first sets out what is at stake, what its vision is, and what the problems are. Future actions will be based on four pillars:

- A cross-sectoral governance framework for data access and use;
- Investments in data and strengthening of Europe's capabilities and infrastructures for hosting, processing, and using data, interoperability;
- Empowerment of individuals, investing in skills and in SMEs;
- Common European data spaces in strategic sectors and domains of public interest.

The strategy sets out key actions in each pillar. For this year, the Commission announced, inter alia, proposals on a Digital Services Act and a European Democracy Action Plan, a review of the eIDAS regulation, and measures to strengthen cybersecurity by developing a Joint Cyber Unit.

The Commission has invited the public to give feedback on its data strategy. The [public consultation](#) is open until 31 May 2020. (TW)

### EDPB: Data Protection Guidelines on Video Surveillance

At its 17th plenary meeting on 28/29 January 2020, the European Data Protection Board (EDPB) adopted [guidelines on the processing of personal data through video devices](#). The guidelines take into account a prior public consultation on the topic (see [eucrim 2/2019, p. 105](#)).

These guidelines examine how the GDPR applies in relation to the processing of personal data by video devices and

how consistent application of the GDPR can be ensured in this regard. The examples are not exhaustive, but the general reasoning can be applied to all potential areas of use. They cover both traditional video devices and smart video devices.

The EDPB highlights that the intensive use of video devices has massive implications for data protection. It also affects citizens' behaviour. In particular, the technologies can limit the possibilities of anonymous movement and anonymous use of services. While individuals might be comfortable with video surveillance set up for a certain security purpose, for example, guarantees must be taken to avoid misuse for totally different and – for the data subject – unexpected purposes (e.g., marketing purpose, employee performance monitoring, etc.). The huge amount of video data generated, combined with new technical tools to exploit images, increase the risk of secondary use. Furthermore, video surveillance systems in many ways change the way professionals from both the private and public sector interact. The growing implementation of intelligent video analysis has contributed to high-performance video surveillance. These analysis techniques can be either more intrusive (e.g., complex biometric technologies) or less intrusive (e.g., simple counting algorithms). The data protection issues raised in each situation may differ, as will the legal analysis when one or the other of these technologies has been used.

In addition to privacy issues, there are also risks related to the possible malfunctioning of these devices and the biases they may produce. According to the guidelines report, research studies found that software used for facial identification, recognition, and analysis performs differently based on the age, gender, and ethnicity of the person, and algorithms are based on different demographics. Thus, bias is one of the major problems of video surveillance; data controllers must regularly assess the relevance of such identification methods and su-

pervise the necessary guarantees. The EDPB ultimately stresses that “video surveillance is not by default a necessity when there are other means to achieve the underlying purpose.”

The guidelines address the lawfulness of processing, including the processing of special categories of data, the applicability of the household exemption, and the disclosure of footage to third parties. Other analysed items include:

- Processing of special categories of data;
- Rights of the data subject;
- Transparency and information obligations;
- Storage periods and erasure obligations;
- Technical and organisational measures;
- Data protection impact assessment.

[The EDPB](#) – an assembly of the EEA data protection authorities and the European Data Protection Supervisor – works on consistent application of data protection rules throughout the European Union and promotes cooperation between the EU’s data protection authorities. (TW)

### Corona Outbreak and Data Protection

The outbreak of COVID-19 and subsequent initiatives and policy measures have triggered many crucial privacy and data protection law issues. The VUB Law, Science and Technology Society Research Group has provided a [collection of statements and materials](#) on tracking initiatives and on European/international resources on the pandemic at its website.

In a [statement of 19 March 2020](#), the European Data Protection Board (EDPB) provides an answer to several questions on data protection in the context of the fight against the COVID-19 pandemic. The statement focuses on the processing of personal data by both public health authorities and employers. The EDPB refers to EU data protection rules and stresses that the GDPR does not, in general, hinder restrictions of freedom

in this emergency situation; however, these measures must be proportionate and limited to the emergency period. Under certain circumstances, the GDPR allows the processing of personal data in the interest of public health without the individual’s consent. The EDPS statement also serves as a reminder of the core principles relating to the processing of personal data.

For the processing of electronic communication data, such as mobile location data, the e-Privacy Directive additionally applies. In this context, public authorities should first aim to process location data in an anonymously (i.e., processing data should be aggregated in a way that individuals cannot be re-identified). This could enable the generation of reports on the concentration of mobile devices at a certain location (“cartography”). If it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the Member States to introduce legislative measures pursuing national security and public security. Such emergency legislation is possible under the condition that it constitutes a necessary, appropriate, and proportionate measure within a democratic society. If these measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals using electronic communication services the right to judicial remedy. The proportionality principle also applies. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved. (TW)

### Victim Protection

#### Commission Announces New Victims’ Rights Strategy

On the occasion of the European Day for Victims of Crime on 22 February 2020 and following the xenophobic/racist attacks in Hanau/Germany on 19 February 2020, Commission Vice-President *Věra Jourová* and Commissioner for Justice *Didier Reynders* [announced a new](#)

[Commission strategy for victims’ rights \(2020–2024\)](#) by summer 2020. According to the Commissioners, 75 million people fall victim to crime every year across Europe. Although the EU has robust victims’ rights legislation in place, there are still too many victims whose rights are not equally guaranteed when a crime is committed in an EU country other than their own. The EU must therefore aim to guarantee equal rights, regardless of where in the EU a person falls victim to a crime.

The new victims’ rights strategy will:

- Empower victims;
- Strengthen cooperation and coordination between national authorities;
- Improve protection and support to victims;
- Facilitate access to compensation.

Support and protection of victims is currently ensured by the EU through the Victims’ Rights Directive (2012/29/EU), sector-specific regulations (e.g., protection of victims of human trafficking, child sexual abuse/child pornography, and terrorism), and a legal scheme that facilitates access to compensation in situations where the crime was committed in an EU country other than the victim’s country of residence. (TW)

### Freezing of Assets

#### CJEU: Confiscation of Illegal Assets via Civil Proceedings Possible

EU law does not preclude national legislation, which provides that a court may order the confiscation of illegally obtained assets following proceedings that were not subject either to a finding of a criminal offence or, a fortiori, the conviction of the persons accused of committing such an offence. The CJEU drew this conclusion in [Case C-234/18 \(ARGO IN 2001\)](#), following a reference for preliminary ruling by the Sofia City Court, Bulgaria. The Bulgarian court is conducting civil proceedings against BP and others for the confiscation of illegally obtained assets. BP, the chair of the



supervisory board of a Bulgarian bank, allegedly incited others to misappropriate funds belonging to that bank in the sum of approximately €105 million. The criminal proceedings against him have not been finally concluded and are still pending. Independent of these criminal proceedings, the Bulgarian Commission responsible for combatting corruption and for confiscating assets brought civil proceedings before said civil court in Sofia. The Bulgarian Commission requested ordering the confiscation of assets from BP and members of his family, because it found that they had acquired assets of considerable value whose origin could not be established. The Bulgarian court asked the CJEU whether such legislation is in line with Council [Framework Decision 2005/212/JHA](#) of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property, i.e., whether civil confiscation procedures can be concluded without first establishing the commission of a criminal offence.

In its [judgment of 19 March 2020](#), the CJEU confirmed the Bulgarian legislation. The CJEU pointed out the purpose of the Framework Decision. It aims at obliging Member States to establish common minimum rules for the confiscation of crime-related instrumentalities and proceeds in order to facilitate the mutual recognition of judicial confiscation decisions adopted in criminal proceedings. This does not preclude Member States from providing other means of confiscation, such as the ones in the case at issue, which are civil in nature. Coexistence with a confiscation regime under criminal law is possible.

The CJEU concludes that EU law does not preclude national legislation which provides that a court may order the confiscation of illegally obtained assets following proceedings which are not subject either to a finding of a criminal offence or, a fortiori, the conviction of the persons accused of committing such an offence. (TW)

## Cooperation

### European Arrest Warrant

#### CJEU Ruling in Spanish Rapper Case: Legislation at Time of Offence Is Decisive

On 3 March 2020, the Grand Chamber of the CJEU decided the legal question referred to by the Court of Appeal of Ghent, Belgium in the extradition case against rapper *Valtònyc* (Case C-717/18).

Spain had issued a European Arrest Warrant against *Josep Miquel Arenas* (who performs as rapper under the name *Valtònyc*) for the purpose of executing a 2017 sentence of imprisonment. He was, inter alia, sentenced to the maximum prison sentence of two years for “glorification of terrorism and the humiliation of the victims of terrorism.” The sentence followed the law in force at the time the offences were committed

(in 2012/2013); however, the maximum term of imprisonment was changed to three years in 2015. The question now was which point in time is decisive in order to determine the “minimum maximum threshold” in Art. 2(2) FD EAW. Art. 2(2) FD EAW does away with the verification of double criminality, inter alia for “terrorism,” under the condition that the offence is punishable in the issuing State for a maximum period of at least three years. For the background of the case and the opinion of the Advocate General, see [eucrim 4/2019, pp. 245–246](#).

Contrary to the opinions of the Belgian and Spanish governments and the Belgian Procureur-generaal, the CJEU ruled that the executing authority must take into account the law of the issuing State in the version applicable to the facts giving rise to the case in which the EAW was issued. The purpose of the FD EAW, which is to facilitate and ac-

### EPRS Study on European Arrest Warrant

In February 2020, the European Parliamentary Research Service (EPRS) published an [in-depth analysis on implementation of the European Arrest Warrant](#) (authors: *Wouter van Ballegooij and Ivana Kiendl Krišto*). The analysis is designed to support an [own-initiative implementation report](#) by the EP’s LIBE committee (rapporteur: *Javier Zarzalejos*, EPP, Spain) and to feed discussions on possible revision of the 2002 Framework Decision on the European Arrest Warrant that may be triggered in 2020. The February report will be followed by a study (planned for April 2020) that will present conclusions on implementation of the framework decision and tentative recommendations on how to address any shortcomings identified.

The analysis observes that the FD EAW is generally recognised as a successful instrument; however, its application has triggered a number of problems:

- Definition of “issuing judicial authorities” and their independence from government;
- The proportionality of EAWs issued for “minor offences” and before the case was “trial ready”;
- Verification of double criminality, its compatibility with the principle of mutual recognition, and the need for further approximation of laws;
- Interplay of the FD EAW with the FD on the transfer of prisoners in the cases of surrender of nationals/residents;
- Application of the “trials *in absentia*” exception;
- The role of the executing authority in safeguarding the fundamental rights of the requested person.

The analysis also deals with the difficulties experienced by requested persons in effectively exercising their procedural rights in accordance with the EU directives setting out the approximation of criminal procedure in EAW cases. (TW)

celerate judicial cooperation, as well as the context of the provision justify this interpretation. The CJEU further argues that making reference to the version of the law at the time of the issuance of the EAW means that the executing authority has to look into possible amendments of the laws in the issuing State, which would run counter to the principle of legal certainty.

Lastly, the CJEU clarifies the relationship between Art. 2(2) and Art. 2(4) FD EAW: the fact that the offence at issue cannot give rise to surrender without verification of the double criminality of the act, pursuant to Art. 2(2), does not necessarily mean that execution of the EAW has to be refused. The executing judicial authority is responsible for examining the double criminality criterion of the act set out in Art. 2(4) in the light of the offence at issue.

The judgment means that the Belgian extradition court must now verify whether the facts giving rise to the EAW against the rap artist would also be punishable under Belgian law. However, the first instance court already denied the double criminality of the act at issue, so it is likely that *Valtònyc* will not be surrendered to Spain. Another solution would be that Spain withdraws the EAW because it was apparently issued on false legal assumptions. (TW)

### MEPs: Revision of EAW Would Open Pandora's Box

On 20 February 2020, MEPs discussed policy options for the European Arrest Warrant in a meeting of the LIBE committee. Legal experts reported on implementation of the Framework Decision on the European Arrest Warrant (FD EAW). Politicians could also draw on a [study by the European Parliamentary Research Service](#) (EPRS) that provided a first in-depth analysis on implementation of the EU's surrender scheme (see separate news item). The EAW instrument was considered a generally successful tool; however, challenges remain. These involve the detention conditions in some

EU Member States, mutual trust among Member States, and interpretation of the 2002 Framework Decision as such. MEPs pointed out that, after 18 years of existence, the FD EAW still triggers a number of CJEU judgments interpreting its provisions in a more or less fundamental way. They are not eager to revise the FD, however, because this would open “Pandora's box” and the achievements would (again) be at stake.

Notwithstanding, the representative from the European Commission announced readiness to revise the FD EAW. Problems are mainly seen in the implementation of the FD and its incorrect application.

The FD EAW will be at the centre of further policy discussions in 2020. The EPRS will present another study on the EAW in April 2020. This will serve as the basis for drafting an own-initiative report by the EP on the EAW implementation. The Commission envisages presenting an in-depth assessment on the EAW by summer. And the upcoming German Council Presidency will put the issue of revision of the EAW on its JHA agenda. (TW)

### Fair Trial Concerns: German Court Suspends Execution of Polish EAW

With its [decision of 17 February 2020](#), the Higher Regional Court (HRC) of Karlsruhe, Germany set aside an extradition arrest warrant against a Polish national who was to be surrendered to Poland via an EAW issued for the purpose of criminal prosecution. The court argued that a fair trial for the requested person is not guaranteed in Poland following recent reforms that had an impact on the disciplinary regime of the judiciary in Poland.

#### ► Background

The court in Karlsruhe refers to the CJEU's judgment of 25 July 2018 in *Celmer* ([Case C-216/18 PPU](#) – also dubbed “LM”), in which the judges in Luxembourg concluded that the executing authority can refrain from giving effect to an EAW under certain circum-

stances on the grounds that the right to a fair trial will not be respected in the issuing EU Member State (see details in [eucrim 2/2018, pp. 104–105](#)).

#### ► *Decision of the HRC*

The court in Karlsruhe extensively dealt with the recent reforms in Poland, which further restrict the independence of judges by introducing, *inter alia*, new rules on the disciplinary regime to the Polish judiciary. This “muzzle law” came into force on 14 February 2020 (for details, consult the recent news on the rule-of-law situation in Poland in the category “Foundations > Fundamental Rights”). The court also took into account recent developments against the Polish reform at the EU level. It paid particular attention to the CJEU's judgment of 19 November 2019, in which doubts were raised as to the independence and impartiality of the new Disciplinary Chamber at the Polish Supreme Court (see details in [eucrim 3/2019, pp. 155–156](#)). It also took into consideration other (pending) infringement actions against the reform that had been referred to the CJEU by the European Commission.

Since the defendant put forward material supporting the assertion that there are systemic deficiencies in the rule of law in Poland, the HRC examined the real risk of breach of the fundamental right to a fair trial – the second step required by the CJEU in the *Celmer* judgment. As this real risk could not be excluded, the HRC sent a catalogue with comprehensive questions to the Polish Ministry of Justice asking for further clarifications on the new muzzle law and its impact on the concrete criminal proceedings, including possible disciplinary measures against the deciding judges. At the same time, the HRC set aside the extradition arrest warrant in Germany – following the current developments in Poland in respect of the judicial reform – because a “high probability” exists that extradition would be inadmissible (at least) at the moment.

### ► Put in Focus

The HRC of Karlsruhe rendered a landmark decision. It is the first time that a court in an EU Member State denied extradition because of possible fair trial infringements in another EU country. Until now, courts in Europe consistently refused to accept non-extradition, following the judicial reforms in Poland that started in 2015, because the hurdles set by the CJEU in *Celmer* could not be overcome. Nearly all cases failed because the courts were not convinced that the requested person would run a real risk of fair trial infringement in Poland. The HRC of Karlsruhe justifies its change in view because the recent muzzle law has shown that the person concerned could run this real risk. It is no longer an abstract danger, because the new disciplinary regime has repercussions on the entire judiciary, including on judges at the competent criminal courts of first instance. However, the HRC of Karlsruhe stresses that the extradition procedure in Germany is not yet finished; a final decision on the case rests on the reply to the catalogue of questions by the Polish authorities.

The decision of the HRC also demonstrates that the judiciary in other EU Member States cannot assess fair trial issues at the level of the European Arrest Warrant without looking at other developments in judicial reform, in particular concrete CJEU case law following infringement proceedings against the reform. The question is also whether the CJEU's case law on the EAW, on the one hand, and on the judicial reform in Poland, on the other, is consistent.

In the present context, the following statement of the Parliamentary Assembly of the Council of Europe is worth reading:

“The Assembly notes that the concerns about the independence of the Polish judiciary and justice system, as well as Poland's adherence to the rule of law, directly affect Europe as a whole. The questions about the independence of the justice system and the respect for

the rule of law are therefore not to be considered as internal issues for Poland. The Assembly calls upon all Council of Europe member states to ensure that the courts under their jurisdiction ascertain in all relevant criminal cases – including with regard to European Arrest Warrants – as well as in relevant civil cases, whether fair legal proceedings in Poland, as meant by Art. 6 of the European Convention for Human Rights, can be guaranteed for the defendants” (No. 11 of the adopted [resolution of 28 January 2020](#)).

The reference number of the HRC's decision (*Beschluss*) of 17 February 2020 is: Ausl 301 AR 156/19. See also [the press release](#) by the Oberlandesgericht Karlsruhe and the summary by [Anna Oehmichen in “beck-aktuell”](#) (both in German). A first analysis in English has been provided by [Maximilian Steinbeis on Verfassungsblog.de](#). (TW)

### Updated Overview on Position of Public Prosecutors in Relation to the EAW

On 30 March 2020, Eurojust published a new version of its [country-by-country overview](#) on the position of public prosecutors in relation to the European Arrest Warrant (EAW) (for the previous version, see [eucrim 2/2019, p. 110](#)). The overview was compiled following the CJEU's judgment of May 2019, in which it declared that the German public prosecutors' offices do not fall within the concept of “issuing judicial authority” in the sense of Art. 6(1) FD EAW due to lack of independence (cf. [eucrim 1/2019, pp. 31–33](#)). In another judgment of May 2019 as regards the Lithuanian Prosecutor General, the CJEU set out requirements of objectivity and independence and the need for effective judicial protection that must be afforded to the requested persons if an EAW is issued by a public prosecutor's office. The judgments raised uncertainties amongst practitioners regarding the legal position of public prosecutors in the Member States.

Alongside an updated summary of

the most recent CJEU judgments taken on this issue in 2019 (see also [eucrim 3/2019, p. 178](#), and [eucrim 4/2019, pp. 242, 244–245](#)), Eurojust's update now also offers information on the UK and Norway as well as information on judicial protection and the possibility to contest a prosecutor's decision to issue an EAW. (CR)

### Financial Penalties

#### CJEU Rules on Union-wide Enforcement of Fines against Legal Persons

**spot light** After its judgment on the interpretation of the Framework Decision on the application of the principle of mutual recognition to financial penalties ([FD 2005/214/JHA](#)) of 5 December 2019 (see [eucrim 4/2019, pp. 246–247](#)), the CJEU delivered another important judgment on the cross-border enforcement of fines on 4 March 2020 ([Case C-183/18, Bank BGŻ BNP Paribas](#)). The reference for preliminary ruling was brought up by a Polish court. In the case at issue, the District Court of Gdańsk, Poland, has to deal with a request from the central judicial recovery office of the Netherlands (CJIB) to recognise and enforce a fine of €36 imposed on the *Bank BGŻ BNP Paribas Gdańsk*, because the driver of a vehicle belonging to the bank had exceeded the authorised speed limit in Utrecht (Netherlands).

#### ► Legal Problems

The referring court first observed that the *Bank BGŻ BNP Paribas Gdańsk* has no legal personality under Polish law and does not have the capacity to act as a party in judicial proceedings. It is a separate entity of the parent company *Bank BGŻ BNP Paribas S.A.*, which has its seat in Warsaw. By contrast, Dutch law covers organisational units like the bank in Gdańsk under the concept of “legal persons” who can be liable for misdemeanours.

Second, the Polish court argues that

there is no legal basis for recognising and enforcing the imposed fine, because the provisions of the Polish Code of Criminal Procedure transposing FD 2005/214 do not include legal persons. Although Art. 9 para. 3 of the FD imposes the obligation to enforce financial penalties against legal persons, even if the executing State does not recognise the principle of criminal liability of legal persons, in the view of the court, an interpretation of the Polish law in conformity with the provision of Art. 9 para. 3 FD would be *contra legem*.

#### ► Questions Referred

As a consequence, the *District Court of Gdańsk* asked the CJEU the following questions:

■ Must the concept of “legal person” in the FD 2005/214 be interpreted in accordance with the law of the issuing State or the executing State or as an autonomous concept of EU law, and which consequences does this answer have for the concrete liability of the banking entity in Gdańsk?

■ Must the financial penalty imposed on a legal person in the Netherlands be enforced in a Member State that has no national provisions on the execution of financial penalties imposed on legal persons?

#### ► Decision as to the First Question

Drawing on the context and the purpose of FD 2005/214, the CJEU concluded that the concept of “legal person” cannot be interpreted as an autonomous concept but must be interpreted in light of the law of the issuing State. The CJEU does not consider the legislation itself problematic but rather the implementation of the FD in practice. It advises the Polish court to consider whether, under the given circumstances, the infringement committed by the bank in Gdańsk can be attributed to the parent company Paribas with its seat in Warsaw. The sanction can be regarded as having been imposed on the entity with a legal personality. As a result, the fine could be enforced against *Bank BGŻ BNP Paribas S.A.*

#### ► Decision as to the Second Question

As regards the conflict between the national law and the obligations under Art. 9 para. 3 FD 2005/214, the CJEU first reiterates its established case law on the effects of Union acts and the principle of uniform interpretation. Referring to the *Poplawski* judgment (see [eucrim 2/2019, pp. 110–111](#)), the CJEU recapitulates that, although the framework decisions cannot have direct effect, their binding character nevertheless places an obligation on national authorities to interpret national law in conformity with EU law as from the date of expiry of the period for the transposition of these framework decisions. While the premise has its limits, e.g., no interpretation *contra legem*, the referring court must exhaust all possibilities to consider an interpretation of the Polish law in conformity with Union law (here, the obligation under Art. 9 para. 3 FD 2005/214). Contrary to the opinion of the referring court, the CJEU believes that the concepts of the Polish Code of Criminal Procedure can be interpreted as referring to the entity on which a final financial penalty has been imposed, regardless of whether this entity is a legal or natural person.

#### ► Put in Focus

Although it is up to the national court alone to determine whether national law can be interpreted in conformity with EU law, the CJEU stressed that national courts are empowered to pull out all the stops in order to ensure compatibility with the wording and purpose of EU law (here the framework decision). The CJEU has thus applied the lessons learned in the context of the European Arrest Warrant (judgment in Case C-573/17, *Poplawski II*) to another instrument of mutual recognition in criminal matters, i.e., the mutual recognition of financial penalties. Against this background, the present judgment in *Bank BGŻ BNP Paribas* is of general significance, because the CJEU applies basic principles of its established case law on the primacy of Union law. (TW) ■

## Law Enforcement Cooperation

### EDPB: CoE E-Evidence Legislation Must Ensure Strong Data Protection Safeguards

In view of the negotiations on a Second Additional Protocol to the CoE Cybercrime Convention (Budapest Convention), which will include a framework for law enforcement authorities to directly receive data from service providers, the European Data Protection Board [addressed a letter to the responsible CoE committee](#) calling for the integration of strong data protection safeguards. The EDPB points out that the contents of the additional protocol deal with sensitive issues of data protection; it will involve the collection of personal data, including not only subscriber but also traffic data, on the basis of orders from another jurisdiction. The new legal framework must be consistent with the [CoE data protection convention](#) (CETS no. 108) and should also be compliant with the EU’s primary and secondary law. The EDPB also called on the CoE committee to ensure transparency of the ongoing discussions. The concerns of the data protection authorities must be taken seriously.

Alongside the CoE, the EU is also working on a new regime for simplified and expedited access to e-evidence following a Commission proposal of April 2018. For the discussion, see [eucrim 3/2019, p. 181](#) with further references. For the state of play of the proposal, see the [EP’s Legislative Observatory website](#). In parallel, the EU is also negotiating an e-evidence agreement with the USA (see [eucrim 4/2019, p. 248](#) with further references). The USA has already established an e-evidence legal framework via its CLOUD Act. *Andrea Jelinek*, the Chair of the EDPB, stressed that the establishment of a modernised instrument for the exchange of personal data with third countries for fighting cybercrime is not only consistent with the Council of Europe *acquis*, but also fully compatible with the EU Treaties and the Charter of Fundamental Rights. (TW)