eucrim
2021 / 2
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Legal effects of COVID-19
Les conséquences juridiques découlant de la Covid-19
Rechtliche Auswirkungen der Corona-Pandemie

2021/2 ISSUE / ÉDITION / AUSGABE

The Associations for European Criminal Law and the Protection of Financial Interests of the EU is a network of academics and practitioners. The aim of this cooperation is to develop a European criminal law which both respects civil liberties and at the same time protects European citizens and the European institutions effectively. Joint seminars, joint research projects and annual meetings of the associations' presidents are organised to achieve this aim.

Contents

News*

Articles

* The news items contain Internet links referring to more detailed information. These links are embedded into the news text. They can be easily accessed by clicking on the underlined text in the online version of the journal. If an external website features multiple languages, the Internet links generally refer to the English version. For other language versions, please navigate using the external website.

Guest Editorial

Dear Readers,

Corruption is extremely flexible and easily adaptable to new scenarios, such as the COVID-19 pandemic. It is generally a major impediment to prosperity and security because it hinders sustainable economic growth, distorts market competition, undermines the rule of law, and erodes trust between citizens and governments. In times of emergency and crisis, however, the risk increases that corruption can exacerbate these negative effects, thwarting efforts geared towards a sustainable and resilient recovery. Corruption therefore has an even more debilitating effect during a *global* pandemic, which enormously challenges societies and economies – it becomes a "thief of the future."

The G20 has played a significant role in global anticorruption efforts. Its Anti-Corruption Working Group (ACWG), established at the Toronto Summit in 2010, was especially designed to prepare "comprehensive recommendations for the consideration of Leaders on how the G20 can continue to make a valuable contribution to international efforts in the fight against corruption." This mandate was intended to ensure that its member countries lead the international community by example and make a qualified contribution to international anti-corruption objectives and instruments. In its ten years of activity, the G20 ACWG has adopted seven Action Plans, ten Accountability Reports, fifteen sets of High-Level Principles, and six Compendia of Good Practices; they contribute to develop the global agenda toward a new era of enforcement.

The work of the ACWG, which includes a multi-stakeholder approach, has been guided by a multiannual Action Plan that systematically takes up commitments by G20 countries to, *inter alia*, (1) support, and implement the UN Convention against Corruption; (2) criminalise and prosecute foreign bribery; (3) cooperate with other countries to trace, prosecute, and repatriate the proceeds of corruption; (4) combat money laundering; and (5) promote integrity in public and private sectors.

G20 countries have been proactive in their response to the COVID-19 pandemic, both at the national level and within the ACWG. These efforts resulted, *inter alia*, in a *Compendium of good practices on anti-corruption in response to COVID-19*. With this compendium, the ACWG seeks to leverage the experience of all G20 countries to create a first vision of best practices against corruption taken during the pandemic. The compendium draws on best practices already developed to combat corruption in procurement fraud and other areas. It aims to provide guidance on national anti-corruption responses and procedures implemented in the G20 states and to provide useful information on countries' responses to the current pandemic in order to prepare for similar future events.

Giovanni Tartaglia Polcini

The priorities of the Italian Presidency of the ACWG for 2021 are ambitious and innovative in terms of content. They focus particularly on modern forms of corruption that are increasingly linked to economic and organised crime. Moreover, they address the development of reliable indicators to measure corruption and to enhance prevention in exposed sectors and new risk areas, e.g., sports. Emphasis has been put on the role of reliable indicators, since measurement indices based on the perceived level of corruption have gradually shown inherent limitations since analyses of the phenomenon have turned out to be too subjective.

The Italian Presidency is highly aware of the new challenges of corruption and the ensuing need for an effective global fight against corruption, stressing the importance of taking into account the challenges posed by COVID-19. On one hand, the response has been to tackle more than just the negative impact of corruption on economic growth, once highlighted by G20 leaders in the High-Level Principles on corruption and growth adopted in Brisbane in 2014. On the other hand, consensus must be reached on a new set of High-Level Principles on integrity and transparency in case of future emergencies. Countries should be prepared and more resilient against any form of corruption beyond the medical crisis.

Giovanni Tartaglia Polcini
Chair of the G20 Anti-Corruption Working Group

News

Actualités / Kurzmeldungen*

European Union

Reported by Thomas Wahl (TW), Cornelia Riehle (CR), and Anna Pingen (AP)

Foundations

Fundamental Rights

Parliament Adopts Resolution on Commission's 2020 Rule of Law Report

On 24 June 2021, the European Parliament (EP) adopted its Resolution on the Commission's 2020 Rule of Law Report. For the report →eucrim 3/2020, 358–359.

MEPs welcomed the Commission's first annual Rule of Law Report and encouraged its continuation in order to identify risks for fundamental rights and the rule of law in the EU. They expressed their satisfaction that the report contains country-specific chapters and called on the Commission to further engage with national governments and national parliaments as well as with civil society and other national actors. The Commission should further intensify country visits so that broader engagement and dialogue with national authorities and civil society can be achieved.

The Resolution welcomed the fact that all Member States are scrutinised according to the same indicators and methodology but emphasised that the Commission should distinguish between systemic breaches of the rule of law and individual, isolated breaches. In future, a more analytical report should be drafted in order to facilitate country-specific recommendations on how to address the encountered concerns.

Monitoring of the independence, quality, and efficiency of the Member States' justice systems is generally welcomed; however, parliamentarians expressed concerns regarding the deterioration of the independence of some Member States' justice systems and the increasing lack of compliance with EU law. They sharply criticised the situation in Poland and Hungary, including the political pressure put on courts to prevent national judges from referring questions to the CJEU about the EU's judicial independence requirements.

The deterioration of media freedom and media pluralism in some Member States is another issue of concern, and the Resolution notes an increasing amount of physical, psychological, and other forms of aggression towards journalists. The EP calls for a broader scope to be applied in future rule-of-law reports, including the values of democracy and fundamental rights. It also calls for clear, country-specific recommendations on how to address the concerns identified. (AP)

Parliament Criticises Informal Agreements on Border Control, Fight against THB, and Return/Readmission of Irregular Migrants

On 19 May 2021, the European Parliament adopted a report making recommendations on human rights protection within the framework of the EU's external asylum and migration policy. The Parliament criticised the practice of the EU and several Member States that have been entering into an increasing number of informal agreements with third countries since 2016 in order to strengthen their operational capacities as regards border control and the fight against human trafficking. It highlighted that these informal agreements neither guarantee a predictable policy nor provide any coherent statutory framework on irregular migration. MEPs also criticised the use of these informal agreements with third countries with respect to the return and readmission of irregular migrants, arguing that these informal agreements lack safeguards ensuring the rights of third-country nationals. The Parliament therefore urged the Commission to sign readmission agreements with third countries which would replace these informal agreements and called out the lack of

* Unless stated otherwise, the news items in the following sections (both EU and CoE) cover the period 1 April – 30 June 2021. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

effective judicial remedies for asylum seekers whose rights may have been violated. (AP)

Poland: Rule-of-Law Developments April – June 2021

This news item continues the updates in previous eucrim issues on the rule-of-law situation in Poland as far as it relates to European law (→*inter alia*, eucrim 1/2021, 4 and eucrim 4/2020, 257):

■ 6 May 2021: In the infringement proceedings in Case C-791/19 concerning the new disciplinary regime for judges within the Polish Supreme Court, Advocate General (AG) *Tanchev* recommends that the Polish legislation does not comply with Union law. The AG shares the points raised by the European Commission that the disciplinary regime casts severe doubts about judicial independence. The possibility of being sanctioned in disciplinary proceedings on account of the contents of decisions exerts particular pressure on Polish judges and impairs their ability to make substantive decisions and to submit questions for preliminary rulings to the CJEU. In addition, the doubts about the independence and impartiality of the Disciplinary Chamber were justified because of the questionable political influence by the National Council of the Judiciary and the Minister for Justice. The provisions of the Disciplinary Code on the competences and the composition of the disciplinary tribunal are thus incompatible with the guarantee under Art. 19 para. 1 subpara. 2 TEU on effective legal protection of rights. Already in April 2020, the Grand Chamber of the CJEU ordered interim measures in this case, according to which the activities of the Disciplinary Chamber of the Supreme Court were to be suspended for the time being due to the questionable provisions of the Polish judicial reform (→eucrim 1/2020, 4).

■ 7 May 2021: For the first time, the European Court of Human Rights (ECtHR), delivers a judgment on the contentious judicial reform in Poland. In the case of Xero Flor w Polsce sp. z o.o. v. Poland (application no. 4907/18), the ECtHR finds that the election of judges to the Polish Constitutional Court in 2015 was irregular and thus infringed the applicant's right to a "tribunal established by law" in accordance with Art. 6(1) ECHR. The judges in Strasbourg criticized that a judge sat at the bench of the Constitutional Court although his seat had been already legally filled by the old Sejm (the Polish parliament). They point out that, after the elections in 2015, the authorities neglected relevant Constitutional Court judgments with a view of usurping the Constitutional Court's role as the ultimate interpreter of the Polish Constitution and the constitutionality of law. The case concerned a complaint from a Polish company that sought compensation from the State for one of its products before the Polish courts.

■ 10 May 2021: In a press release, the ECtHR announces that it would examine in detail five more cases related to the controversial Polish judicial reform (for other cases pending before the ECtHR, →eucrim 2/2020, 68). The cases concern the suspension of applicants as judges or public prosecutors from their official duties as well as a complaint against the contentious nomination of judges by the National Council of the Judiciary. The ECtHR requested from the Polish government to submit its observations on the cases. In addition, the ECtHR announced that all current and future applications concerning complaints about various aspects of the reform of the judicial system in Poland will be given priority (so-called Category I cases). In accordance with the Court's prioritisation policy, this level of priority is assigned to urgent cases.

■ 20 May 2021: Advocate General *Bobek* considers the amended Polish practice, according to which the Minister for Justice (who is simultaneously the General Prosecutor) has unfettered discretion to second judges to higher courts, is in clear breach of Art. 19 para. 1, subpara. 2 TEU, read in conjunction with Art. 2 TEU. The national measures at issue appear highly problematic in view of both external and internal aspects of judicial independence. According to the AG, it is worrisome if the criteria for secondment of judges are not made public, the seconded judges seem not subject to ordinary rules, and their secondment is for an indeterminate period of time and can be terminated at any moment at the discretion of the Minister of Justice. In addition, impartiality and judicial independence are at risk if the Minister for Justice/General Prosecutor, i.e. wearing a "double hat", is the body that designates judges and if designated judges may hold the position of "disciplinary agents", as it is the case pursuant to the Polish provisions. The AG's opinion was triggered by a reference for preliminary ruling from a single judge at the Regional Court of Warsaw (Joined Cases C-748/19 to 754/19). The judge casted doubts that the composition of the panel of judges in criminal proceedings before the Regional Court still observes the presumption of innocence and the separation of powers due to the possible influence on both the public prosecutor's office and the judge to the disadvantage of the accused.

■ 20 May 2021: It becomes known that the Polish Prime Minister *Mateusz Morawiecki* submitted an over 100-page-long application to the Polish Constitutional Court which should determine whether certain provisions of the TEU concerning the primacy of EU law and effective judicial protection are consistent with the Constitution of the Republic of Poland. An unofficial English translation is provided for at the portal <https://ruleoflaw.pl>.

■ 15 June 2021: The Polish Constitutional Court blatantly rejects a request filed by the Polish Ombudsman to remove judges from the court's bench as reaction to the ECtHR's judgment of 7 May 2021 in *Xero Flor w Polsce sp. z o.o. v. Poland* (see above). According to an English translation of the decision at the website <https://ruleoflaw.pl>, the Polish Constitutional Court considers

the ECtHR's judgment "a non-existent judgment (*sententia non existens*)." The Polish judges believe that "the ECtHR judgment of 7 May 2021 … is based on arguments testifying to the Court's ignorance of the Polish legal system, including the fundamental constitutional assumptions specifying the position, system and role of the Polish constitutional court. To this extent, it was issued without legal grounds, overstepping the ECtHR's jurisdiction, and constitutes unlawful interference in the domestic legal order, in particular in issues which are outside the ECtHR's jurisdiction."

■ 17 June 2021: According to Advocate General (AG) *Bobek*, a national court is entitled to disregard national legal provisions on the attribution of jurisdiction or rulings of a higher court if it considers them incompatible with EU law, in particular with the principle of judicial independence. The AG's opinion concerns a legal battle between the Polish bar association and the Polish General Prosecutor/Minister of Justice, in which the former has refused to initiate disciplinary proceedings against a lawyer. The referring Disciplinary Court of the Bar Association in Warsaw wondered which procedural consequences are triggered by the CJEU's judgment of 19 November 2019 that confirmed that the Disciplinary Chamber of the Supreme Court lacks judicial independence (→eucrim 3/2019, 155–156). The Disciplinary Chamber will, upon possible appeal, finally adjudicate on the disciplinary sanctions of the lawyer. AG *Bobek* backs the opinion that the EU Service Directive (2006/123/EC) is applicable in the proceedings at issue and may secure unlawful withdrawal of lawyers' authorizations. Lastly, the AG notes that references for preliminary rulings may not be the appropriate way to tackle pathological situations in a EU Member State. He believes that infringement actions remain a more appropriate remedy to settle institutional stand-offs in a context where one or more actors refuse to follow the CJEU's judgments. The case is referred to as C-55/20 (*Ministerstwo Sprawiedliwości).* (TW)

Hungary: Recent Rule-of-Law Developments

This news item continues the overview of recent rule-of-law developments in Hungary. For reports in previous issues →eucrim 1/2021, 4–5; and eucrim 4/2020, 257–258; and eucrim 3/2020, 162–163 with further references.

■ 21/26 May 2021: The Hungarian Helsinki Committee (HHC) releases two information notes on the creation of parallel state structures by the Hungarian government. The first note relates to the state's financing of public universities by public trust funds. The second note deals with the creation of new managerial and regulatory powers to one single supervisory, government-sponsored authority in the areas of tobacco retail, judicial enforcement, gambling, and liquidation.

■ 3 June 2021: The CJEU dismisses an action by Hungary seeking annulment of the European Parliament's resolution of 2018, which triggered the procedure for determining a clear risk of a serious breach – by a Member State – of the values on which the European Union is founded (procedure of Art. 7 TEU). Hungary argued that the EP did not count the abstentions among the votes cast when adopting the resolution, which required a two-thirds majority. Hungary put forth that only counting the votes cast in favour and against the resolution, while excluding the abstentions, is not in line with Art. 354 TFEU and Rule 178(3) of the EP's Rules of Procedure. The CJEU holds Hungary's action for annulment pursuant to Art. 263 TFEU admissible but unfounded (Case C-650/18). The CJEU notes that the concept of "votes cast" in Art. 354 para. 4 TFEU is not defined in the Treaties but invites autonomous interpretation in accordance with the usual meaning of the concept in everyday language. As a result, this concept covers only the casting of a positive or negative vote on a given proposal, whereas abstention is understood as a refusal to adopt a position at all and cannot be treated in the same way as a "vote cast." Consequently, the rule laid down in Art. 354 para. 4 TFEU must be interpreted as precluding abstentions from being taken into account. The CJEU follows the opinion of AG Bobek presented on 3 December 2020.

■ 15 June 2021: The Hungarian parliament passes the "Anti-Paedophilia Act". Besides introducing heavier penalties for sexual offences against minors, the ruling Fidesz party made last-minute amendments to the bill that sparked controversy all over Europe. The legislation passed also stipulates several bans that critics find a violation of freedom of expression and LGBTQI+ rights. According to the law, it is forbidden to:

- Make available content to minors featuring portrayals of homosexuality or sex reassignment;
- Promote homosexuality or sex reassignment when educating students;
- Broadcast advertisements that portray or promote "deviation from the identity corresponding to one's sex at birth, sex reassignment, or homosexuality."

The Hungarian government defended the bill by arguing that it is not discriminatory and aims only at protecting children. NGOs criticised that "this move endangers the mental health of LGBTQI youth and adults, and inhibits them from accessing information and support in a timely manner for preventive purposes." They also pointed out that the new law is part of a series of measures that curtail the rights of LGBTQI people and have been stigmatizing them since 2018. The new law has triggered harsh criticism by the EU.

■ 23 June 2021: European Commission President *Ursula von der Leyen* calls the passed Hungarian anti-paedophilia bill "a shame", which "goes against all the fundamental values of the European Union." Her staff will send a formal letter to the Hungarian government to clarify the content of the anti-paedophilia legislation.

■ 24 June 2021: 17 heads of state or government sign a joint letter in the margin of the EU summit in which they pledge to "continue fighting against discrimination towards the LGBTI community". Although the letter does not name Hungary expressly, it is clearly targeted at the Hungarian anti-paedophilia law. Dutch Prime *Minister Mark Rutte* said at the summit that, with the LGBT law, "Hungary has no place in the EU." Luxembourg's Prime Minister *Xavier Bettel* commented that Mr *Orban* was wrong to conflate homosexuality with paedophilia within the law. Germany's chancellor *Angelika Merkel* condemned the act as "wrong". According to civil rights organisations in Hungary, it remains to be seen how the law will be enforced, since the legal definitions are apparently unclear. (TW)

Rule-of-Law Developments in other EU Countries

Beyond Poland and Hungary, a close eye is also being kept on other EU countries as regards upholding the value of the rule of law. Recent developments concern Malta, Romania, and Czechia. For a more detailed report on these events, please refer to the online publication of this news item dated 8 July 2021. (TW)

Reform of the European Union

Launch of the Digital Platform "Conference on the Future of Europe"

19 April 2021 marked the launch of the multilingual digital platform "Conference on the Future of Europe" (→eucrim 1/2021, 5–6). It provides a unique opportunity for European citizens to engage in the debate about the future of Europe and to exchange views with experts and EU institutions until spring 2022. The launch marks a big step forward in the integration process. Commission President *Ursula von der Leyen* has called all European citizens to participate in shaping "the Europe they want to live in." Participation is open to every European citizen, and the engagement of young Europeans is especially encouraged.

The Conference aims to create a new public forum in order to stimulate an open and transparent debate with all European citizens on a variety of topics, such as climate change, the environment, a stronger economy, social justice, the rule of law, and security

The ideas and comments on these topics will be published on the platform and feed into discussions taking place in European Citizens' Panels and Plenaries. European Citizen's Panels will discuss different issues that are of crucial importance for the EU's development, and the Conference Plenaries will make sure that the Panels' recommendations are being debated freely. During the conference, several decentralised events will take place next to the European Citizens' Panels and Conference Plenaries. The final outcomes of the conference will then be presented to the Joint Presidency in a report and examined by the European Parliament, the Council, and the European Commission. (AP)

Security Union

Council Conclusions: Impact of COVID-19 on Internal Security

On 7 June 2021, the JHA Council adopted conclusions "on the impact of the COVID-19 pandemic on internal security: threats, trends, resilience and lessons learned for EU law enforcement." By stressing that the COVID-19 pandemic posed unpredictable risks and threats to the internal security landscape, the conclusions mainly recommend to make better use of the existing instruments. They call on the Member States and the EU institutions to step up efforts in order to ensure protection, achieve better preparedness, and reinforce prevention. Member States should do the following:

■ Better coordinate the exchange of cross-border information, joint law enforcement operations, best practices and expertise between neighbouring countries;

■ Prevent hindrances to strategical, operational and tactical cross-border law enforcement cooperation, in particular in case of travel restrictions;

■ Develop and promote information and awareness campaigns for their citizens, focusing particularly on the prevention of cybercrime, misinformation, and hate speech;

■ Develop scenario-based training and practical exercises within CEPOL (the EU agency for law enforcement training) to ensure preparedness and resilience for future pandemics and other crises;

■ Share best practices on reporting channels for victims of crime, such as domestic violence and sexual abuse.

Europol is encouraged to support Member States through the exchange of information that affect internal security in crisis situations and to develop best practices from its analytical reports on crime trends and risk assessments during the current COVID-19 pandemic. The Commission should support Europol and the innovation lab to set up a common, resilient and secure instrument for communications in the EU law enforcement cooperation framework.

It should be noted that the conclusions come along with conclusions on the impact of COVID-19 on terrorism and violent extremism that were adopted at the same JHA Council meeting (→separate news item under "Terrorism") (TW)

Parliament Calls for Tighter EU Cybersecurity Standards for Connected Products and Associated Services

On 10 June 2021, the European Parliament (EP) adopted a resolution on the EU's Cybersecurity Strategy for the Digital Decade in order to make connected products and associated services secure by design, resilient to cyber incidents, and able to be quickly patched if vulnerabilities are discovered. While MEPs welcomed the Commission's plans for horizontal legislation on cybersecurity requirements for connected

products and associated services, they also stressed the need for the Commission to harmonise national laws in order to avoid fragmentation of the Single Market. The EP called for promotion of the development of secure and reliable networks/information systems, infrastructure, and connectivity across the Union.

The Commission is now called on to assess the need for a proposal on a regulation introducing cyber-security requirements for applications, software, embedded software, and operating systems by 2023. In addition, MEPs emphasised that outdated applications, software, embedded software, and operating systems no longer receiving regular patches and security updates constitute a significant share of all connected devices and a cyber-security risk – this issue therefore needs to be included in the Commission's proposal.

The MEPs acknowledged that the COVID-19 crisis has further exposed cyber-vulnerabilities in several critical sectors, e.g., healthcare, and the number of cyber-attacks on healthcare systems is on the rise. The resolution cautioned that the use of hybrid threats (including the use of disinformation campaigns and cyber-attacks on infrastructure) is increasing and that they risk affecting democratic processes, such as elections, legislative procedures, law enforcement, and the administration of justice. The lack of agreement on cyber-intelligence collaboration at the EU level and the lacking collective response to cyber- and hybrid attacks are also cause for concern. (AP)

Area of Freedom, Security and Justice

Brexit: EP Formally Approves TCA and Requests its Involvement in Implementation

In its plenary session of 27 April 2021, the European Parliament (EP) consented to the conclusion of the Trade and Cooperation Agreement (TCA) between the European Union and the United Kingdom. The deal received an overwhelming majority of 660 out of 697 votes cast. To minimise disruption, the agreement has been provisionally applied since 1 January 2021 (→eucrim 4/2020, 265). The EP's consent was necessary so that the TCA can enter into force permanently. The period of provisional application ends on 30 April 2021.

In addition to the vote on the TCA, MEPs adopted a resolution that sets out the EP's evaluation of and expectations from the EU-UK Agreement. The resolution passed by 578 to 51 votes, with 68 abstentions. MEPs welcomed the conclusion of the EU-UK Trade and Cooperation Agreement that limits the negative consequences of the UK's withdrawal from the EU. However, they consider Brexit a "historic mistake" and recall that "a third country cannot have the same rights and benefits as a Member State." They also stress that the goals pursued by the EP have been largely achieved by the TCA. This achievement is, *inter alia*, ensured through an enforceable level playing field (including for state aid, social and environmental standards), a long-term settlement on fisheries, an economic agreement which will mitigate many of the negative consequences of the UK's withdrawal from the EU, and a new framework for justice, police and internal security cooperation based on full respect for the ECHR and the EU's data protection legal framework. The EP regrets nonetheless that the UK was not willing to extend cooperation to important areas, such as foreign and security policy and participation in the student exchange programme Erasmus+. Furthermore, it is regrettable that judicial cooperation in civil matters was not part of the negotiations for the future partnership between the EU and the UK.

MEPs criticise that the TCA was hastily negotiated which impacted the democratic oversight of the final text ahead of the provisional application. They underline that the EP must play a full role in the monitoring and implementation of the Agreement, which must include, for instance, the EP's involvement in unilateral EU actions under the Agreement or the taking into account of the EP's views regarding the implementation of the TCA by both parties.

The resolution sets out the EP's viewpoint on the various chapters and topics of the TCA. Regarding issues in connection with the area of freedom, security and justice and the protection of the EU's financial interests (in detail summarised at eucrim 4/2020, 265–271) the following points raised can be highlighted:

- The Commission should remain vigilant on questions of taxation and money laundering, where all available tools such as the listing processes should be used to dissuade the UK from adopting unfair practices;
- A decision of the adequacy of the UK's data protection framework must be in line with the CJEU case law, should not be taken rashly and cannot be the object of negotiation between the UK and the EU;
- The part on law enforcement and judicial cooperation in criminal matters with the UK is of an unprecedentedly close nature with a third country;
- The suspension and termination mechanism in relation to law enforcement and judicial cooperation is to be welcomed, in particular the ECHR conditionality;
- The EU should keep an eye on UK practices that may develop harmful tax schemes (including in UK Crown Dependencies and Overseas Territories where the TCA does not apply) or impact the financial stability of the EU;
- The UK must respect its financial commitments under the TCA that ensure the protection of the EU's financial interests;
- Strong cooperation on VAT and customs duties is needed in order to ensure proper collection and the recovery of claims; cooperation must include swift

exchange of information among the customs authorities and the fight against VAT and customs fraud;
- The implementation of the control mechanisms must be ensured, including the right of access of Commission services, the ECA, OLAF and the EPPO;
- Both parties must continue their (regulatory) common protection of intellectual property rights. (TW)

Brexit: EP Criticises Commission's Draft Adequacy Decisions

In a resolution adopted on 21 May 2021 with a narrow majority of 344 against 311 votes, the European Parliament found that the European Commission's assessment of the UK data protection law and practice is incomplete and inconsistent with the CJEU's requirements for adequacy decisions. In February 2021, the Commission tabled two drafts for adequacy decisions (→eucrim 1/2021, 7). They confirm the UK having an equivalent level of data protection to that of the EU – a precondition for future transfers of personal data both between private entities and between law enforcement authorities in accordance with the GDPR and Directive 2016/680. MEPs call on the Commission to address the concerns raised in the resolution and to amend the draft implementing decisions. The resolution mainly raises the following concerns:
- Lack and often non-existent enforcement of the GDPR by the UK when it was an EU Member State;
- Too broad exceptions from fundamental data protection rights, in particular in immigration law and for purposes of national security;
- No sufficient reaction by the UK yet as regards the use of mass surveillance data;
- Insufficient adequacy status as regards onward transfers, which can lead to the bypassing of the EU rules on data transfers to countries or territories not deemed adequate under EU law;
- Persistent concerns over UK's data retention regime.

MEPs call on national authorities to suspend data transfers to the UK if guarantees are not included. If necessary, the Member States must conclude no-spy agreements with the UK. MEPs also share the opinions by the European Data Protection Board (EDPB) of April 2021 that identified deficiencies in the draft adequacy decisions and required further improvements. (TW)

Brexit: Commission Rejects UK Application to Join Lugano Convention

With Brexit and the end of the United Kingdom's EU membership, the 2007 Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano Convention) no longer applies to the United Kingdom of Great Britain and Northern Ireland (UK). On 8 April 2020, the UK applied to accede to the Lugano Convention. On 4 May 2021, the Commission rejected – in a communication to the European parliament and the council – the entry of the UK to the Convention. The Convention had originally been concluded between the European Union, Denmark, and the European Free Trade Association (EFTA) states of Switzerland, Norway and Iceland to regulate international jurisdiction and the recognition and enforcement of foreign judgments in civil and commercial matters.

In its communication, the Commission justified the rejection of the UK's application by stating that the Lugano Convention is a flanking measure of the EU's internal market and embedded in the EU-EFTA/EEA context. In relation to all other third countries, the EU promotes cooperation within the framework of the multilateral Hague Conventions. Due to the Brexit, the status of the UK has been derogated to that of a third country without a special link to the internal market. Any future cooperation between the UK and the EU in matters of civil judicial cooperation will therefore be regulated by the Hague Conventions. (AP)

Recent JHA-Relevant Infringement Procedures

On 9 June 2021, the Commission presented information about the opening and progress of several infringement procedures in the area of justice and home affairs / security law and PIF. For a more detailed report on these procedures, please refer to the online publication of this news item dated 1 July 2021. (TW)

CCBE: Position Papers

On 26 March 2021, the Council of Bars and Law Societies of Europe (CCBE) held an online Standing Committee during which several position papers with relevance to the Area of Freedom, Security and Justice were adopted:
- The CCBE adopted its comments on the Communication on the Digitalisation of Justice in the EU. The Communication was published on 2 December 2020 by the European Commission, with the intent to improve the digitalisation of justice in the EU. With regard to the refusal of many national authorities to verify electronic signatures from other Member States, the CCBE stressed the importance of an effective application of the eIDAS regulation that had been adopted on 23 July 2014. Calling for reinforcement of EU-wide legal certainty, the CCBE also emphasised the need for EU-wide minimum standards, which would ensure that national e-justice systems can guarantee the right to a fair trial.
- The CCBE welcomed the European Commission's e-CODEX proposal for a regulation on a computerised communication system in cross-border civil and criminal proceedings. The CCBE voiced concerns, however, over the lack of clear and concrete provisions regarding the operating conditions of access points in the e-CODEX proposal, especially on "how to maintain the integrity of the system when entities operating access points are private companies." The CCBE called the proposal inadequate regarding the protection of fundamental rights, noting that there should

be explicit references to the applicability of the Charter of Fundamental Rights of the EU.

■ The CCBE adopted its Contribution for the Rule of Law Report 2021. In this contribution, the CCBE pointed out that lawyers are faced with many challenges during the Covid-19 pandemic and its consequences for access to justice, quality of justice, and upholding the rule of law. In this regard, the CCBE urged the Commission to continue monitoring such developments and to take necessary actions to prevent any undermining of the rule of law. The CCBE also reaffirmed the importance of recognising lawyers as key actors in the justice system – on the same level as judges and prosecutors.

■ The CCBE adopted its comments on the European Judicial Training Strategy. It welcomed the Communication of the Commission "Ensuring justice in the EU – a European judicial training strategy for 2021–2024" and especially the European Judicial Training strategy, which promotes a common rule-of-law culture upholding fundamental rights. The CCBE stressed the importance of the objective to train 15% of lawyers in EU law by 2024 but pointed out that adequate funding is needed in order to meet such an ambitious goal. (AP)

Schengen

Commission Strategy for a Stronger and More Resilient Schengen Area

On 2 June 2021, the Commission presented its new strategy for a fully functioning and resilient Schengen area. With this strategy, the Commission is aiming to make the Schengen area – the largest visa-free zone in the world – stronger and more resilient, accentuating that the free flow of people, goods, and services is at the heart of the European Union. The Commission acknowledged that the Schengen area has been under a lot of pressure in recent years, facing new challenges stemming from the 2015 refugee crisis, persistent terrorist threats and terrorist attacks on European soil, and the COVID-19 pandemic. These new challenges have led some Member States to reinstate internal border controls.

In order to successfully face these challenges and continue reaping the benefits that the Schengen area provides, the strategy aims to achieve the following goals:

(1) Improve the EU's external border management

The Commission will present:

■ A proposal for a Regulation on digitalisation of the visa procedure;

■ A proposal for a Regulation on digitalisation of travel documents and facilitation of travel by 2023;

■ A recommendation to Member States on the exchange of information/on situational awareness to be used in bilateral and multilateral agreements with third countries (model provisions).

(2) Reinforce the Schengen area internally

The Commission will:

■ Improve police cooperation with an EU Police Cooperation Code that will provide a coherent EU legal framework to ensure that law enforcement authorities have equal access to information held by other Member States;

■ Reinforce the automated exchange of important data categories relating to Prüm Council Decisions;

■ Expand the use of advance passenger information (API) to also cover intra-Schengen flights;

■ Update the European Arrest Warrant (EAW) Handbook.

(3) Increase preparedness and enhance governance

The Commission will:

■ Continue to organise regular Schengen Forums in order to discuss the situation of Schengen at the political level and to foster continued reflection and cooperation;

■ Relaunch the adoption of the "State of Schengen Report";

■ Propose an amendment to the Schengen Borders Code by the end of 2021 in order to address the lessons learned from the COVID-19 crisis (e.g., the reintroduction of internal border controls) and to deal with any future Schengen-wide challenges;

■ Codify the guidelines and recommendations developed in relation to COVID-19 in the Practical Handbook for Border Guards.

The Commission calls upon the Council to take the necessary steps for Bulgaria, Romania, and Croatia to become part of the Schengen area without controls at the internal borders of Member States.

On the same day the new strategy was presented, the Commission also proposed a regulation on the establishment and operation of an evaluation and monitoring mechanism to verify application of the Schengen *acquis* and repealing Regulation (EU) No 1053/2013, in order to foster common trust in implementation of the Schengen rules. (AP)

Second Schengen Forum

After the first Schengen Forum meeting in November 2020 (→eucrim 4/2020, 272–273), the political dialogue on strengthening the Schengen rules has continued. The Schengen Forum convenes members of parliament and home affairs ministers with the aim of fostering cooperation and political dialogue as well as of building up stronger confidence in the Schengen rules.

The second Schengen Forum was opened on 17 May 2021 with a keynote speech by *Ylva Johansson*, Commissioner for Home Affairs. *Johansson* stressed that, with the COVID-19 pandemic and the ensuing lockdowns, the EU and the Schengen area were under a lot of pressure and strain. She pointed out, however, that these challenging times can also be seen as an opportunity for the Schengen community to be reminded of how important Schengen is for the mobility of EU citizens and for the EU economy.

The challenges have also shown that there is a need for more cooperation and

coordination as well as for better use of new technology in external border management and by European police forces in order to reinforce the Schengen area. According to *Johansson*, the pandemic has shown that proportionate and coordinated border control measures are usually more effective than unilateral and uncoordinated action taken by individual Member States. Even if rigid controls at internal borders can be justified in acute emergencies, they should be seen as an exception, as they are neither proportionate nor effective. In order to build a more secure Schengen area, the Commissioner also stressed the importance of the launch of the European Travel Authorisation System (ETIAS, →eucrim 2/2018, 82, 84). She announced that the Commission intends to present an Annual State of Schengen Report, which will serve as a basis for a better Schengen evaluation. (AP)

Legislation

Commission Proposes Artificial Intelligence Act

spot light

On 21 April 2021, the Commission tabled a proposal for a regulation laying down harmonised rules on artificial intelligence (AI). Following the Commission's White Paper on AI from 2020 (→eucrim 1/2020, 8–9) and in a new step aiming to turn Europe into the global hub for trustworthy AI, the proposal strives to balance the numerous risks and benefits the use of AI can provide.

In order to implement the second objective of the White Paper addressing the risks associated with using AI in certain contexts, the Commission is proposing a legal framework that will enable the benefits the use of AI has to offer to be reaped, while simultaneously upholding the EU's values and fundamental rights. The Regulation on AI pursues four objectives:

- To ensure that AI systems placed on the EU market are safe and in line with existing EU law on fundamental rights and values;
- To ensure legal certainty when facilitating investment in and innovation into AI;
- To enhance governance and effective enforcement of the existing law on fundamental rights and safety requirements applicable to AI systems;
- To facilitate the development of a single market for lawful, safe, and trustworthy AI applications and to prevent market fragmentation.

The direct application of the new rules across all Member States will be based on a future-proof definition of AI that is based on a risk-based approach, going from *unacceptable-risk* to *minimal-risk* AI systems:

- AI systems that are considered an unacceptable risk, i.e., a clear safety threat to people and "contravening Union values," will be banned. The Commissions sees such unacceptable risks in AI systems that allow "social scoring" by governments.
- AI systems that are identified as high-risk, i.e., posing significant risks to the health and safety or fundamental rights of persons, will be put under strict obligations before being placed on the European market. This includes AI systems that are being used, for example, in critical infrastructures, migration, asylum and border control management, or in the administration of justice and democratic processes. The Commission stresses that all remote biometric identification is considered high-risk and will therefore be subject to specific restrictions and safeguards.
- Limited-risk systems, i.e., chatbots, will be subject to minimum transparency obligations.
- Minimal-risk AI systems that represent only a minimal or no risk for the rights and/or safety of citizens, i.e., spam filters, are not subject to the proposed Regulation.

On the governance side, the proposal establishes a European Artificial Intelligence Board at the EU level, which is to be tasked with contributing to effective cooperation between the national supervisory authorities and the Commission and with providing advice and expertise to the Commission.

In parallel to the first worldwide initiative to set up a legislative framework on AI, the Commission presented the following documents:

- The Communication "Fostering a European Approach to Artificial Intelligence", which summarises the EU's policy on AI and explains the "AI package";
- An updated "Coordinated Plan" on AI, which defines joint actions for the European Commission, the Member States, and private parties in order to turn the EU into a global leader of trustworthy AI;
- A proposal for a regulation on machinery products, which ensures that the new generation of machinery guarantees the safety of users and consumers and encourages innovation. (AP)

EDPB/EDPS Joint Opinion on Commission's AI Proposal: Call for Ban of Biometric AI Surveillance

On 18 June 2021, the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) adopted a joint opinion on the European Commission's Proposal for a regulation laying down harmonised rules on artificial intelligence (AI). The EDPB and the EDPS welcomed the Commission's proposal that had been presented on 21 April 2021 (→news item above). They made clear that it has important data protection implications.

The EDPB and the EDPS further welcomed the extension of the proposal to the provision and use of AI systems by EU institutions, bodies or agencies (EUIs). They criticised, however, the exclusion of international law enforcement cooperation from its scope.

Regarding the risk-based approach to AI systems, the EDPB and the EDPS stressed that the concept of "risk to fundamental rights" should be aligned with the General Data Protection Regulation

(GDPR). The proposal should explicitly address the rights and remedies available to individuals affected by AI systems.

The EDPB and the EDPS were also critical of the Commission's exhaustive list of high-risk AI systems, which might create a black-and-white effect undermining the overall risk-based approach. They agreed with the proposal in that the classification of an AI system as "high-risk" does not necessarily mean that it is still lawful *per se* and can be deployed by the user as such.

Regarding the prohibition of the use of certain AI systems, the EDPB and the EDPS recommended that intrusive forms of AI – such as those AI systems intended to be used by law enforcement – be prohibited AI systems under Art. 5 of the proposal, instead of simply being classified as "high-risk" in the annex. They particularly anticipate that the use of remote biometric identification of individuals in publicly accessible spaces may create an especially high-risk of intrusion into individuals' private lives. They therefore called for a stricter use of such AIs, e.g. a general ban on any use of AI for automated recognition of human features in publicly accessible spaces (e.g., recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals) in any context. They also endorsed a ban AI systems using biometrics to categorize individuals into clusters based on ethnicity, gender, political or sexual orientation, and any other grounds on which discrimination is prohibited under Art. 21 CFR.

Despite welcome the designation of the EDPS as the competent market surveillance authority for the supervision of the EUIs, its role and tasks need further clarification. They embraced the proposal for the establishment of the "European Artificial Intelligence Board" (EAIB). However, they feel that the future AI Regulation should give more autonomy to the EAIB, in order to allow the Board to truly ensure the consistent application of the Regulation across the single market.

Regarding transparency issues, the opinion recognised that ensuring transparency in AI systems is a very challenging goal. The registration of high-risk AI systems in a public database in order to provide information about the application and the flaws of AI systems would be welcomed. (AP)

EDPS Comments on Commission's Artificial Intelligence Act Proposal

In a press release dated 23 April 2021, the European Data Protection Supervisor (EDPS), *Wojciech Wiewiórowski*, welcomed the Commission's proposal for a new regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act →separate news item above). The EDPS especially recognised the merit of a risk-based approach concerning the future-proof definition of AI that the Commission adopted in its proposal.

The EDPS also stressed the importance of a ban on remote biometric identification in the public and expressed his regret that the previous calls for a moratorium on the use of remote biometric identification systems in publicly accessible spaces have not been addressed by the Commission. *Wiewiórowski* remarked that the use of remote biometric identifications that results in automatic recognition of human features in public spaces could present "extremely high risks of deep and non-democratic intrusion into individuals' private lives". For the discussion on a ban of AI technology enabling biometric mass surveillance (→eucrim 1/2021, 10).In order to support the Commission in strengthening the protection of individual rights, the EDPS will analyse the proposal of the new regulation. (AP)

Justice Ministers Debate on DSA

Following the Commission proposal on a Digital Services Act (DSA) – presented in December 2020 (→eucrim 4/2020, 273–274) – the ministers of justice of the EU Member States held a debate on the plans to combat illegal content online at the JHA Council meeting on 7 June 2021. The debate mainly focused on the aspects related to orders to providers from national authorities to act against illegal content or to provide information, as well as the obligation of large providers to notify authorities of suspicions of serious criminal offences. Ministers particularly stressed:

- The freedom of expression must be ensured when restrictions are enacted;
- Regarding the orders from national authorities, it must be clarified that the DSA does not conflict with other JHA instruments;
- Regarding the notification obligations for providers, the DSA must clarify the concepts of "serious criminal offence involving a threat to life or safety of persons" and the "promptness" of reaction. (TW)

Commission Gives Guidance on Strengthening the Code of Practice on Disinformation

On 26 May 2021, the Commission released a Communication entitled "Guidance on Strengthening the Code of Practice on Disinformation." The Commission stressed that the COVID-19 pandemic has illustrated the problem posed by disinformation as well as the increasing importance of digital technologies in everyday life.

With this guidance document, the Commission wants to strengthen the Code of Practice on Disinformation and address gaps and shortcomings in digital communication in order to create a more transparent, safe, and trustworthy online environment. The Commission called the Code of Practice on Disinformation – in effect since October 2018 – a centrepiece of the EU's efforts in the fight against disinformation. The Code is a self-regulatory tool that is employed by major online platforms and trade associations. It provides a structured framework in which the private entities monitor and improve their policies on disinformation (→eucrim news item of 11 January 2020).

However, the Communication also identified the Code's shortcomings, as revealed by an assessment in 2020. This includes, for instance, inconsistent and incomplete application of the Code across platforms and Member States, limitations intrinsic to the self-regulatory nature of the Code, and gaps in the coverage of the Code's objectives commitments. In order to address these shortcomings, the Commission calls for the following improvements:

- Stronger commitment by signatories to ensure a more effective response to the spread of disinformation;
- Wider participation in the Code by established and emerging platforms, online services which disseminate information to the public (e.g., smaller social media and search services), and stakeholders from the advertising ecosystem beyond the circle of the Code's current signatories;
- Tailored commitments that correspond to the diversity of services provided by signatories and the particular roles they play in the advertising ecosystem;
- Reinforcement of cooperation between the Member States, the signatories of the Code, and the European Digital Media Observatory (EDMO);
- Strengthened commitments aimed at no longer funding the dissemination of disinformation in signatories' own services or on third-party websites;
- Strengthened commitments from the Code's signatories to enhance the transparency and public disclosure of political ads;
- Comprehensive disclosure of current and emerging forms of manipulative behaviour used to spread disinformation;
- Extension of cooperation with fact-checkers on the part of signatories;
- Empowerment of users by facilitating a better understanding of the functioning of online services and the use of tools that foster more responsible behaviour online;
- A framework for robust access to platform data by the research and fact-checking community and adequate support for their activities;
- Release of regular reports by signatories under the reinforced monitoring framework using harmonised templates, including sets of standard and auditable formats providing data against the key performance indicators (KPIs).

The Commission's Guidance is also designed to develop the existing Code of Practice into a co-regulatory instrument, as foreseen under the Digital Services Act (DSA). (AP)

Parliament Approves Interinstitutional Agreement on Mandatory Transparency Register for Lobbyists

On 27 April 2021, the European Parliament adopted a decision on the conclusion of an interinstitutional agreement between the European Parliament, the Council of the European Union, and the European Commission on a mandatory transparency register. The text was adopted with 645 votes in favour, five votes against, and 49 abstentions. It shall enhance the transparency of the EU decision-making process and foster the accountability of the EU institutions.

The adopted text brings major changes to the already existing Transparency Register, making it mandatory for interest representatives to register themselves before carrying out certain lobbying activities (see Annex A to the Agreement) relating to any of the three signatory institutions (the European Parliament, the Council of the European Union, and the European Commission). The Parliament also made clear that the agreement covers indirect lobbying activities, especially since such activities have become more important during the COVID-19 pandemic. (AP)

Commission Seeks to Improve EU Law-Making Process

On 19 April 2021, the Commission adopted a Communication on Better Regulation, aiming to improve the EU's law-making process by simplifying the EU legislation and reducing its burden. The Commission will therefore:

- Invite the Member States, regions, and key stakeholders to remove obstacles and red tape that have been slowing down investments in and building up of a 21st century infrastructure to maximise the benefits of an improved EU law for citizens, businesses, and society as a whole;
- Introduce a "one in, one out" approach adapted to policymaking in the EU. As EU regulations often come with costs, the Commission reiterated that they must remain reasonable and proportionate. In order to reduce the burdens resulting from EU legislation – for both citizens and businesses (especially for small and medium-sized enterprises) –, the principle of "one in, one out" is to ensure that any newly introduced burdens are balanced by removing equivalent burdens in the same policy area;
- Consolidate public consultations into a single "call for evidence" on the "Have Your Say" web portal, which will consist of a description of the initiative and include a link to the public consultation, where relevant;
- Keep respondents who contributed to public consultations informed by publishing a summary report on each public consultation within eight weeks of its closure;
- Increase the transparency of EU law-making by improving portals, such as EU Publications, EUR-Lex, and "Have Your Say", and by improving the links between them;
- Mainstream the UN's sustainable development goals (SDGs) in order to take better consideration of sustainability;
- Integrate strategic and science-based foresight into policymaking, ensuring that decisions taken are grounded in a long-term perspective and are "future-proof."

The Commission stressed that an improvement of the EU law-making process can only be reached by cooperation between local, regional, and national authorities, social partners, and between EU institutions – the European Parliament, the Council, and the Commission. (AP)

Institutions

Council

Programme of the Slovenian Council Presidency (JHA)

On 1 July 2021, Slovenia assumed the EU Council Presidency for the next six months. The motto: "Together. Resilient. Europe." In general, priority topics will be post-pandemic economic recovery, the Conference on the Future of Europe and the EU enlargement process in the Western Balkans.

In the area of justice, Slovenia will focus on the protection of human rights in light of challenges posed by new technologies and the use of internet. Priorities will include combatting hate speech and hate crime, discussions on ethical aspects and the potential impact of the use of AI on fundamental freedoms. Work will continue on e-evidence, e-CODEX and the EU's accession to the European Convention on Human Rights. The Presidency will also prepare a comprehensive response to the EU strategy on rights of children.

In the area of home affairs, the country will strive for ensuring a fully functioning Schengen area and building up more robust Schengen rules. The Presidency intends to make progress in the negotiations on key files in the areas of asylum and migration. Another important priority will be to ensure a high level of security in the EU through enhanced police cooperation between Member States and neighbouring regions such as the Western Balkans. In this context, the proposal to amend the Europol Regulation will be particularly relevant. (TW)

OLAF

Working Arrangement between EPPO and OLAF Signed

spot light

On 5 July 2021, European Chief Prosecutor *Laura Kövesi* and OLAF Director-General *Ville Itälä* signed a working arrangement that sets out the future operational cooperation between the EPPO and OLAF. The agreement can be considered an important milestone since both offices are mandated to fight EU fraud. OLAF conducts administrative investigations, while the EPPO conducts criminal investigations and prosecutes cases falling under its competence before the national courts of the participating Member States. The EPPO Regulation (Council Regulation (EU) 2017/1939) stipulated the relationship between the two bodies only rudimentarily.

The Working Arrangement aims to establish close cooperation between OLAF and the EPPO in the exercise of their respective investigatory and prosecutorial mandates, in particular through the exchange of information and mutual support. It regulates the modalities on the following issues:

- Exchange of information, including reciprocal indirect access to each other's electronic case management system;
- Mutual reporting and transmission of potential cases to each other;
- Mutual support in the course of investigations;
- Conduct of complementary investigations by OLAF;
- Information exchange on trends;
- Joint training exercises and staff exchange programmes.

In addition, the Arrangement sets out the structures for institutional/strategic and operational cooperation, which includes the establishment of contact points. The parties agreed to continuously monitor the functioning of the arrangement and to periodically evaluate its application. (TW)

Operation Silver Axe VI against Illegal Pesticides

On 17 June 2021, OLAF and Europol reported on the results of the annual operation "Silver Axe". The operation, which was coordinated meanwhile for the sixth time, targets the global trade in counterfeit and illegal pesticides. Pesticides are among the most regulated products in the world, thus cheaper illegal and substandard products promise high profits but they can heavily damage the environment.

Operation Silver Axe VI (carried out between mid-January and end of April 2021) led to 12 arrests and the seizure of over 1200 tonnes of illegal pesticides in total. It is estimated that the seized products are worth €80 million. Law enforcement authorities targeted the sale of counterfeits, banned products and unregulated imports – both online and offline. Inspections on land and sea borders, inland marketplaces, parcel service providers and online marketplaces were carried out. Europol reported that the operation showed a trend towards increased online sales. Asian countries remain the main source of illegal pesticides production. The operation involved 35 countries and several supranational institutions, such as the EU Intellectual Property Office (EUIPO) and the European Crop Protection Association (ECPA). OLAF mainly provided expertise in identifying and tracking suspicious movements. These movements are then reported to national customs and plant protection authorities which are able to intercept the suspicious transfers of goods. For previous operations of Silver Axe, →eucrim 2/2020, 81; eucrim 2/2019, 88; and eucrim 2/2018, 85. (TW)

OLAF Activity Report 2020

On 10 June 2021, OLAF published its activity report for 2020. The report highlights that OLAF's work was much marked by the COVID-19 pandemic, when OLAF had to act against fake and substandard medical products which risked floating the EU market especially at the beginning of the pandemic. However, OLAF successfully continued work on other issues affecting the EU's financial interests, such as collusion and manipulation of public procurement and illegal tobacco trade. The key figures regarding OLAF's performance in 2020 are as follows (for activity reports

of previous years, →eucrim 3/2020, 167 and →3/2019, 163):

- OLAF concluded 230 investigations, and issued 375 recommendations to the relevant national and EU authorities;
- OLAF recommended the recovery of over €293 million to the EU budget;
- OLAF opened 290 new investigations, following 1,098 preliminary analyses carried out by OLAF experts.

OLAF also reports on several trends that came up during OLAF's anti-fraud investigations in 2020:

- Manipulations or circumvention of public procurement procedures was often used to hide conflict of interest and demonstrated collusion between beneficiaries and contractors;
- Frauds in farming and rural development funds of the EU continuous to be one of the major fields of investigations, e.g. frauds through false or inflated invoices;
- Fraud in relation to EU research funding remains at high risk;
- Smuggling and counterfeiting tobacco products remains one of the highest concerns in the area of EU revenue – trends in 2020 include the illegal production of cigarettes by criminal networks within the EU and the increase in illegal sales of water pipe tobacco;
- Fraud affecting the environment and biodiversity is growing.

As in previous years, OLAF informs on its coordination role in joint customs operations with EU and international partners, such as SILVER AXE V, OPSON IX and DEMETER VI (which have also been reported in eucrim).

The focus chapter of the 2020 annual report deals with OLAF's role in keeping citizens healthy and safe. OLAF stresses that tackling counterfeit and dangerous goods has been a priority for a long time. However, the COVID-19 pandemic suddenly offered new business opportunities for counterfeiters and fraudsters which required urgent reaction to the risks on the part of OLAF and its partners. Right at the very start of the outbreak, OLAF opened investigations in counterfeit or substandard medical products. Tracking down fake hand sanitisers from Turkey is given as one example where the authorities could prevent a major threat to the citizens health (→eucrim 4/2020, 278). Beyond COVID-related products, OLAF was able to keep away other counterfeit products from European consumers, e.g. by one operation that succeeded in the seizure of 1.3 million litres of wine and alcoholic beverages. The environment is an increasing business area for fraudsters. OLAF participated in actions for example against illicit pesticides and illicit refrigerant gases.

Other topics of the report include:

- OLAF's relations with its partners;
- Monitoring the outcome and impact of OLAF's recommendations to the national authorities and EU bodies;
- Communication;
- Data protection and complaints, including relevant case law from the European Courts.

Ultimately, OLAF outlines its contributions to the EU policy to fight and prevent fraud. In 2020, OLAF continued to work on the development of the new Commission anti-fraud strategy, and took an active role in the new EU Recovery and Resilience Facility.

When presenting the report, OLAF Director-General *Ville Itälä* said: "(…) Indeed, the new opportunities for fraud brought by the virus – in particular the lucrative market for counterfeit or substandard products such as facemasks or hand sanitisers – brought new challenges for OLAF in 2020. I am extremely proud that my OLAF colleagues proved so adept at rising to those challenges, showing resilience, creativity and flexibility to keep on working as normally as possible, keeping European citizens safe despite all the challenges posed by the pandemic." (TW)

Cooperation between OLAF and WCO on New Footing

On 7 June 2021, OLAF Director-General *Ville Itälä* and the Secretary General of the World Customs Organization (WCO), *Kunio Mikuriya,* signed a new agreement enhancing cooperation between the two bodies. The new "Administrative Cooperation Arrangement" widens the scope and operational possibilities of a previous arrangement from 2003. Whereas the 2003 arrangement covered only the exchange of information on tobacco seizures, the new one allows the information sharing on a wider range of fraudulent activities, e.g., counterfeiting and illicit trade in protected species.

The arrangement will also allow closer and more effective cooperation on joint operations. OLAF will be able to share information with the WCO members (customs administrations worldwide) on customs fraud cases (exchange is, however, limited to non-personal data only).

The arrangement follows a last year's agreement between OLAF and the WCO that linked the two main databases of the bodies with regard to tobacco smuggling, i.e. the WCO's Customs Enforcement Network (CEN) database and the Customs Information System (CIS+) managed by OLAF (→eucrim 2/2020, 79–80). (TW)

OLAF Involved in Operation against Eel Trafficking

As indicated in the activity report for 2020 (→news item above), OLAF's role in operations involving the environment and biodiversity, in particular the protection of endangered species, has increased in recent years. On 4 June 2021, OLAF informed the public that it participated, for the first time, in Operation Lake. This annual operation, which started five years ago, targets the smuggling of the protected European eel. The stocks of this endangered species are estimated to have fallen by 90% in recent years and illicit trade with the eel is a very lucrative business, with profits estimated to be up to €3 billion.

Operation Lake V, which took place between November 2020 and June 2021,

involved law enforcement and customs authorities in 16 EU Member States and 8 non-EU countries. Several EU authorities participated as well with Europol leading the operation. Criminal activities of networks mainly origin in France, Spain, Portugal and the United Kingdom – the four European countries producing glass eels. Concealed consignments are then shipped to destinations in Asia where the eel is considered a delicacy and high prices are paid.

OLAF's role consisted primarily in the coordination of the activities of the French customs authorities. The operation was one of the biggest anti-smuggling customs operations in French history involving 20 French customs authorities across the country.

Europol coordinated the overall operational activities, facilitated the information exchange and provided analytical support. During several action days, Europol deployed experts on the field to cross-check operational information in real time against Europol's databases.

In sum, Operation Lake V led to over 58,000 inspections, 52 arrests and the seizure of over 400 kg of eels, valued at approximately €1.2 million. OLAF and Europol stressed that the operation is a vital weapon to fight illegal trade in European wildlife. The authorities also detected new modi operandi used by criminal networks for the eel trafficking. (TW)

OLAF Helps Greek Authorities Seize Nearly 10 Million Contraband Cigarettes

At the end of May 2021, Greek authorities succeeded in seizing almost 10 million contraband cigarettes. The cigarettes were smuggled from China in suitcases. The action prevented the loss of around €2 million in excise duties and VAT. OLAF supported the operation by alerting the Greek authorities when it identified the suspicious shipment. OLAF also closely cooperated with the Chinese Anti-Smuggling Bureau which tipped off the EU body. Cigarette smuggling remains one of the major threats to the EU budget. In 2020 alone, international operations involving OLAF led to the seizure of nearly 370 million illegal cigarettes that would have caused losses of around €74 million in customs and excise duties and VAT to EU and Member State budgets (→eucrim 1/2021, 14). (TW)

European Public Prosecutor's Office

1 June 2021: EPPO Assumes its Investigatory and Prosecutorial Tasks

On 1 June 2021, the European Public Prosecutor's Office (EPPO) started its own investigation procedures. European Chief Prosecutor, *Laura Kövesi*, had proposed 1 June 2021 as the official start date (→eucrim 1/2021, 15). The corresponding Commission decision was published in the Official Journal of the EU on 28 May 2021 (L 188, 100).

On the occasion of its operational start, the EPPO launched a video explaining what the start means for citizens, how the EPPO will work, and how persons can report a crime to the new body. The Commission provided a document with answers to the most important questions on the EPPO's activities.

In a joint statement, Vice-President *Vera Jourová*, Commissioner *Johannes Hahn,* and Commissioner *Didier Reynders* stressed that 1 June 2021 "opens a new chapter in fighting cross-border crime." They also emphasised that the EPPO will play a pivotal role in observing the correct implementation of the NextGenerationEU, the EU's €750 billion funding programme to boost the economy after the COVID-19 pandemic.

The European Data Protection Supervisor (EDPS), *Wojciech Wiewiórowski*, stated that the power to investigate and prosecute crimes against the EU's financial interests also presents new challenges for the EDPS' supervision activities. "The body's multi-layered structure and the interplay between the EPPO Regulation and national provisions implementing the law enforcement directive will require coordination between the EDPS and the national data protection authorities," he said.

European Chief Prosecutor *Laura Kövesi* told reporters that the credibility of the EU depends on the EPPO. "Our decisions will directly affect the fundamental rights of European citizens. We're the first really sharp tool to defend the rule of law in the EU," according to *Kövesi*.

- For the views of the European Chief Prosecutor and the European Prosecutors on the future challenges of the EPPO and their work, as well as on the future perspectives of the fight against fraud, see the special issue of eucrim 1/2021.
- For other articles on the EPPO, see, *inter alia*, the articles in the special issues eucrim 2/2018, eucrim 3/2017, and 2/2012.
- Individual articles have been published in eucrim 4/2020, 310; 1/2020, 36; eucrim 4/2019, 271; 3/2019, 198 and 205; eucrim 1/2019, 66; eucrim 4/2017, 193; eucrim 1/2017, 25; eucrim 2/2016, 94 and 99; and eucrim 3–4/2008, 177 et seq.

The mood has been somewhat marred by the continued lack of European Delegated Prosecutors (EDPs), as Slovenia and Finland have not made appointments. On 4 June 2021, the EPPO announced that an agreement had been reached with the Finnish side on how to manage timely implementation with regard to the Finnish EDPs. On 5 July 2021, the EPPO College approved the appointment of one EDP in Finland.

At the end of May 2021, Slovenia decided to stop the procedure for appointing two EDPs and to launch a new call for tender. This led to the resignation of Slovenian Justice Minister *Lilijana Kozlovič*. Slovenia will take over the EU Council Presidency on 1 July 2021. In a statement on 27 May 2021, *Laura Kövesi* sharply criticised the Slovenian situation. She remarked that "the manifest lack of sincere cooperation of

the Slovenian authorities with the EPPO seriously undermines the trust in the effective functioning of the management and control systems for EU funds in Slovenia."

Currently, 22 EU Member States are applying the EPPO Regulation 2017/1939 by way of enhanced cooperation. Sweden has expressed its interest in joining the EPPO in 2022. Only Hungary, Poland, Ireland, and Denmark are not participating or have opted out.

The first cases referred to the EPPO are from Germany and Italy. The EPPO operational guidelines adopted in April 2021 indicate that a high number of so-called backlog cases must be processed at the start of operational activities. As long as investigations are still ongoing in the respective Member States, the possibility to exercise the right of evocation according to Art. 27 of the EPPO Regulation should only be used if exercise of the EPPO's competence would bring added value to the continuation of the investigation. (TW)

Europol

European Parliament Discussion on New Europol Regulation

Following the Commission's Proposal of 9 December 2020 for a Regulation amending Regulation (EU) 2016/794 (→eucrim 4/2020, 279), European Parliament rapporteur *Javier Zarzalejos* (ES, EPP) published a draft report setting out a possible EP position on the Commission proposal on 10 May 2021. The rapporteur generally welcomes the targeted revision of the Europol Regulation as proposed by the Commission but suggests some amendments. The draft European Parliament legislative resolution focuses on the financial provisions, governance rules, and provisions relating to reporting and evaluation to ensure proper parliamentary scrutiny.

At the end of May 2021, the draft report was discussed in the Committee on Civil Liberties, Justice and Home Affairs (LIBE). and it is currently awaiting the Committee vote. On 2 June 2021, the EP's Committee on Budgets reacted to the Commission Proposal and issued an Opinion revising its budgetary impact. Bar associations also reacted to the Commission's proposal – they took a more critical stance towards the planned Europol reform (→separate news items below). The EDPS raised concerns over the impact of the plan on data protection in his opinion of 8 March 2021 (→eucrim 1/2021, 15–16). (CR)

CCBE Position on Europol Reform

In a position paper issued on 6 May 2021, the Council of Bars and Law Societies of Europe (CCBE) criticised various aspects of the Commission proposal on a reform of current Europol Regulation 2016/794, which was tabled in December 2020 (→eucrim 4/2020, 279). In the paper, the CCBE informs the EU legislator and policy makers about several standards that should be upheld in the Europol Regulation and makes several recommendations:

- Ensuring that the technology used to collect, process, and exchange personal data among private companies and/or law enforcement authorities/Europol does not interfere with the rules on professional secrecy or legal professional privilege;
- Laying down clearer and more precise provisions with regard to the concepts of "national security/extremism/terrorism/crisis" that would justify the exchange of personal data between Europol and private parties according to the proposal;
- Strengthening democratic oversight of Europol's activities by the Joint Parliamentary Scrutiny Group (JPSG);
- Reinforcing the legal remedies that are conferred on data subjects within Europol itself;
- Acknowledging independent judicial supervision at all stages of the procedure if data relating to lawyer-client communication are accessed;
- Incorporating strong safeguards for the transfer of personal data by Europol to private parties, which should include the ban on transferring data protected by professional secrecy or legal professional privilege and the guarantee that data are adequate, relevant, and up-to-date before any transmission is made;
- Refraining from the idea that Europol should take the lead in the development of artificial intelligence (AI) solutions for law enforcement purposes, given the risk of bias and discrimination when using AI tools;
- Defining more clearly the scope of Europol's new research and innovation activities and reconsidering the safeguards and controls on Europol in this field.

Before any further legislation is enacted, the CCBE calls on Europol and the competent European institutions to first tackle the potentially unlawful processing of a vast amount of personal data (as stated by the EDPS in his inquiry decision of autumn 2020 (→eucrim 3/2020, 169)). Given that the current Europol Regulation 2016/794 earmarked a comprehensive evaluation of Europol by May 2022 and given the said admonishment of the EDPS, the CCBE considers the EU legislator's current plan to strengthen Europol's mandate premature and hasty. (TW)

Position Paper of German Bar Association on Europol Reform

In April 2021, the German Bar Association (DAV) published a position paper on the Commission Proposal for a Regulation amending the Europol Regulation (→eucrim 4/2020, 279) that outlines its concerns over the proposed enlarged mandate of Europol. The DAV is especially concerned about allowing Europol to directly exchange personal data with private parties. For the DAV, such competences risk a circumvention of fundamental rights, e.g., prior judicial authorisation, independent control, and effective remedies. Enabling Europol to directly exchange data with private parties may also affect information

Policing in Cyberspace

On 25 June 2021, Europol published a spotlight report entitled "The Cyber Blue Line." It sets out the challenges and issues involved in a growing area of police work dedicated to providing safety and security online. The two authors of the report, *Mary Aiken* (professor of cyberpsychology) and Dr. *Philipp Amann* (Head of Expertise & Stakeholder Management at Europol's European Cybercrime Centre – EC3), take a look at the blurring line between the real and online worlds by asking whether policing should be redefined to accommodate its role in cyberspace. Parameters of law and order may need new concepts to ensure public safety and maintain security and to tackle online dangers, antisocial behaviour, and criminality.

The report is part of a discussion on where law enforcement responsibility lies when it comes to maintaining secure and safe societies in cyberspace. Europol invites academics and think-tanks interested in the topic to get in touch in order to work together to discuss, debate, and conceptualise this "Cyber Blue Line." (CR)

protected by the lawyer-client privilege and by data protection provisions. In this context, the possibility to conduct big data analysis is considered incompatible with the jurisprudence of the ECtHR and the CJEU, according to which the use of personal data is allowed only to the extent of what is strictly necessary.

Lastly, two powers in the proposal are considered incompatible with Art. 88 TFEU:

- Requesting Member States to initiate an investigation without the need of a cross-border element.
- Entering data on suspected involvement of third-country nationals into the Schengen Information System (SIS).

They surpass the Agency's competence given under EU's primary law. (CR)

Eurojust

Further Cooperation between Eurojust and FRA

On 24 June 2021, the President of Eurojust, *Ladislav Hamran*, and the Executive Director of the EU Agency for Fundamental Rights (FRA), *Michael O'Flaherty*, met to discuss potential areas of cooperation and possible common activities in judicial matters. Topics of cooperation ranged from facial recognition technology and detention problems to the access to lawyers and victims' rights. FRA presented its research findings on criminal detention, access to legal advice, and implementation of the EU Directive on combating terrorism. Both agencies also discussed their cooperation in the Victims' Rights Platform. The platform was established in 2020 and brings together actors engaged in victims' rights at the EU level to discuss horizontal issues and to support implementation of the EU Strategy on victims' rights. The impact of the COVID-19 pandemic on cross-border judicial cooperation and the central role of Eurojust in rolling out the Digital Justice Project were also on the agenda. (CR)

Next Steps to Set Up EuroMed Judicial Network of Contact Points

On 27 May 2021, CrimEx members met to discuss the next steps in setting up a EuroMed Judicial Network of Contact Points (EMJNet). CrimEx is a permanent working group composed of judicial experts from Euro-Mediterranean countries.

The planned EMJNet shall be composed of practitioners who can assist with requests for international judicial cooperation in criminal matters. They will strengthen contacts and operational cooperation between criminal justice authorities from the EU Member States and the Southern Partner Countries (SPCs), namely Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, and Tunisia. (CR)

National Member for Romania Reappointed

At the beginning of May 2021, Ms *Daniela Buruiana* was reappointed as National Member for Romania at Eurojust. Ms *Buruiana* served as Senior Prosecutor at the Romanian Prosecution Service before joining Eurojust in 2014. During her first term of office, she chaired Eurojust's Cybercrime Team and her National Desk strongly increased cooperation between Romania and other Member States and third countries. (CR)

Urgent New JIT Funding Possible

In April 2021, Eurojust launched a new scheme for JIT funding that is applicable to urgent and/or unforeseen cross-border operational activities by Joint Investigation Teams (JITs). This funding scheme is being offered in addition to existing funding through annual calls for proposals. The "Funding without Calls for Proposal" scheme aims to provide targeted, short-term grants for activities falling outside the scope of the annual calls for proposals. Applications for these short-term grants may be submitted anytime during the year. All relevant information, application forms and budget forms can be found on the Eurojust website on JIT funding. (CR)

Frontex

New Frontex Operation in Serbia

On 16 June 2021, Frontex launched a new operation in Serbia. 44 standing corps officers from 14 countries helped detect criminal activities:

- Trafficking in human beings;
- Document fraud;
- Smuggling of stolen vehicles, illegal drugs, weapons, and excise goods;
- Potential terrorist threats.

"Joint Operation Serbia – Land 2021" is taking place at Serbia's border to Bulgaria in order to counter the increasing number of illegal border crossings observed in recent years. (CR)

ECA Report on Frontex

On 7 June 2021, the European Court of Auditors (ECA) published a special report analysing Frontex's support to external border management. For the first time, the audit assessed whether Frontex carried out four out of its six primary activities effectively to implement European integrated border management and, in this way, support Member States in preventing, detecting, and responding to illegal immigration and cross-border crime. The four primary activities assessed by the audit concern information exchange, risk analysis, vulnerability assessment, and operational response. The report also examines the preparedness of Frontex to fulfil its new and expanded 2019 mandate.

Overall, the report finds that Frontex's support for Member States/Schengen-associated countries in fighting illegal immigration and cross-border crime is not sufficiently effective. Issues identified by the report include, for instance, problems with information exchange that prevent the agency from providing an accurate, complete, and up-to-date situational awareness of the EU's external border. Although migrant information dispatched by Frontex is timely and relevant, obstacles (such as the lack of information or poor technical standards for border control equipment) undermine the construction of a complete situational picture at the EU's external borders. Additionally, issues of data completeness and quality prevent the agency from providing precise assessments. Other issues identified involve deploying resources to counter cross-border crime and to adapt to the new mandate.

The report sets out the following recommendations to be implemented in 2021 and 2022:

- Improving the information exchange framework and the European situational picture;
- Updating and implementing the Common Integrated Risk Analysis Model (CIRAM);
- Securing access to other sources of information;
- Developing the potential of vulnerability assessment;
- Improving Frontex's operational response;
- Addressing the challenges of Frontex's 2019 mandate.

The ECA points out that the last external evaluation of Frontex's operations was carried out in 2015 and did not include Frontex's mandate as defined in the 2016 Regulation. In 2019, the ECA audited Frontex's return operations in special report No 24/2019 on migration management in Greece and Italy. Later this year, the ECA will issue audit reports on the EU's migrant return policy and on combating migrant smuggling. (CR)

Action against Frontex Brought before the CJEU

On 25 May 2021, three NGOs (frontLex, the Progress Lawyers Network, and Helsinki Monitor) submitted an action against Frontex to the CJEU (General Court). On behalf of two asylum seekers, the NGOs are accusing Frontex of complicity in human rights violations allegedly taking place at Greece's borders. This is an unprecedented legal action, since Frontex is being brought before the EU court for human rights violations for the first time. The lawsuit will likely scrutinize Frontex's involvement in "push-back" operations in the Aegean Sea. (CR)

Tech Foresight on Biometrics

On 14 and 15 April 2021, the first Technology Foresight Workshop on Scenario Analysis was held to explore, analyse, and discuss four socio-techno-economic scenarios for the year 2040 and their possible implications on the development of biometric technologies. The four different future scenarios consisted of fictitious stories ranging from a possible dynamic EU economy in an appeased world to a slow EU economy in a conflictual world. For each scenario, participants discussed what the future of travel, border checks, and biometrics might look like. The event was part of the ongoing "Technology Foresight on Biometrics for the Future of Travel" project, which analyses possible future changes in travel and border checks and potential impacts on the European Border and Coast Guard community. (CR)

Agency for Fundamental Rights (FRA)

Council Approves General Approach to Fundamental Rights Agency Reform

On 5 June 2020, the Commission submitted to the Council a proposal for a Council regulation amending Regulation (EC) No 168/2007 establishing the European Union Agency for Fundamental Rights (FRA). On 7 June 2021, the Council approved a general approach to the new legislation, which will enhance the Agency's mandate and improve its functioning through more efficient procedures. In order to adapt FRA's mandate to the Lisbon Treaty, the Agency's activities should also cover the particularly sensitive fundamental rights area of police cooperation and judicial cooperation in criminal matters. The area of common foreign and security policy will be excluded from the scope. (AP)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

Budget Conditionality: EP Ready to Take Commission to CJEU

The dispute between the European Parliament (EP) and the Commission over the application of Regulation 2020/2092 is entering the next round. Regulation 2020/2092 sets out the rules for the protection of the EU budget from breaches of the rule of law, the so-called budget conditionality mech-

New EU Anti-Fraud Programme

The European Parliament and the Council established the Union Anti-Fraud Programme for the duration of the multiannual financial framework 2021–2027. The underlying Regulation (EU) 2021/785 was published in the Official Journal L 172 of 17 May 2021. The Programme succeeds the Hercule III Programme that ran until 2020.

The Regulation lays down the objectives of the Anti-Fraud Programme, the budget for the period 2021–2027, the forms of Union funding and the rules for providing such funding. The specific objectives are:

- Preventing and combating fraud, corruption and any other illegal activities affecting the financial interests of the Union;
- Giving support to the reporting of irregularities, including fraud, with regard to the shared management funds and pre-accession assistance funds of the Union budget;
- Providing tools for information exchange and support for operational activities in the field of mutual administrative assistance in customs and agricultural matters.

The financial envelope for the entire period will be €181.207 million. The following actions are considered eligible for funding:

- Providing technical knowledge, specialised and technically advanced equipment and effective IT tools enhancing transnational and multidisciplinary cooperation and cooperation with the Commission;
- Enhancing staff exchanges for specific projects, ensuring the necessary support and facilitating investigations, in particular the setting up of joint investigation teams and cross-border operations;
- Providing technical and operational support to national investigations, in particular to customs and law enforcement authorities to strengthen the fight against fraud and other illegal activities;
- Building IT capacity in the Member States and third countries, increasing data exchange and developing and providing IT tools for the investigation and monitoring of intelligence work;
- Organising specialised training, risk analysis workshops, conferences and studies aimed towards improving cooperation and coordination among services concerned with the protection of the financial interests of the Union;
- Any other action laid down in Commission work programmes, which is necessary for achieving the general and specific objectives of the Anti-Fraud Programme. (TW)

anism (→eucrim 3/2020, 174–176). On 23 June 2021, EP President *David Maria Sassoli* wrote to Commission President *Ursula von der Leyen* calling to fulfil the Commission's obligations under said Regulation.

The letter comes in response to an EP resolution of 10 June 2021, in which the MEPs urge the Commission to propose measures under the new rules against the background of ongoing severe violations of the principles of the rule of law in some EU Member States. They criticised that the Commission has not respected the deadline of 1 June 2021 to draw up guidelines on the application of the Regulations as requested in the EP's previous resolution of 25 March 2021 (→eucrim 1/2021, 19). *Sassoli* now set a new deadline: If the Commission does not react within two weeks, the EP will sue the Commission for failure to act in accordance with Art. 265 TFEU.

The EP reiterates its standpoint that the Rule-of-Law Conditionality Regulation is directly applicable in its entirety in all Member States for all funds of the EU budget, including resources allocated through the EU Recovery Instrument, since its entry into force on 1 January 2021. MEPs blame the Commission for not having used all tools at its disposal to address persistent, severe violations of democracy and fundamental rights in the EU, in particular in Poland and Hungary (→eucrim news reports on the recent rule-of-law developments in Poland and Hungary).

The Commission is hesitating to apply the conditionality mechanism because the EU leaders agreed in a political compromise in December 2020 that the guidelines for application of the conditionality mechanism should only be finalised after a ruling of the CJEU in the event of an action for annulment. Hungary and Poland had filed such an action in spring 2021 (Cases C-156/21 and C-157/21, →eucrim 1/2021, 19). The majority of MEPs believe that this political agreement has no legal effect. (TW)

German Federal Constitutional Court Paves Way for EU's Recovery Instrument

In its decision of 15 April 2021 (Ref.: 2 BvR 547/21, a summary is available in English here) the German Federal Constitutional Court (FCC) rejected an application for preliminary injunction against the German Act Ratifying the EU Own Resources Decision. The Council Decision of 14 December 2020 on the system of own resources enables the EU to raise funds of up to €750 billion within the framework of the temporary reconstruction instrument Next Generation EU (→eucrim 3/2020, 174). In particular, it has been designed to help alleviate pandemic-related economic consequences.

The applicants consider the EU approach to be a violation of the German Parliament's budgetary rights and of the overall budgetary responsibility enshrined in the constitutional principle of democracy, which may not be touched as a constitutional core principle pursuant to Art. 79(3) of the Basic Law. Although the FCC does not consider the application in the principal proceedings to be either obviously inadmissible or clearly unfounded, after a summary ex-

amination, it found that a violation of the constitutional identity does not seem very likely. This is justified by the fact that the borrowing of money on capital markets by the EU does not lead to a direct liability for Germany and that such loans are limited in amount, duration, and purpose.

In the context of balancing the consequences, the FCC decided, in view of the limited period of validity and the EU-political relevance of the instrument of reconstruction, that waiting for the principal proceedings would weigh more heavily than a later finding of unconstitutionality.

In the main proceedings, it will now have to be examined, on the basis of an identity control, how far-reaching Germany's liability and budgetary obligations as provided for in the Own Resources Decision are and whether parliamentary influence on the handling of the financial resources has been preserved. If the FCC were to find in the principal proceedings that the 2020 Own Resources Decision constitutes an *ultra vires* act or encroaches upon constitutional identity, it would be incumbent upon the Federal Government, the *Bundestag,* and the *Bundesrat* to restore constitutional order by all means available to them. (TW)

Commission Provides Guidance on Conflicts of Interest

On 7 April 2021, the European Commission published a guidance on the avoidance and management of conflicts of interest under the new 2018 Financial Regulation (FR). The FR, which entered into force on 2 August 2018, has strengthened the measures to protect the EU's financial interests. Strengthened rules on conflicts of interest are now explicitly extended to Member States' authorities (regardless of the Member States' internal governance arrangements) and any person implementing any of the EU funds under shared management. In addition, the definition of conflicts of interest was broadened, now covering "any other direct or indirect personal interest." The guidance pursues the following objectives:

- Promoting a uniform interpretation and application of the rules on avoidance of conflicts of interest for financial actors and staff of the EU institutions involved in implementing, monitoring and controlling the EU budget under direct/indirect/shared management;
- Raising awareness among Member States' authorities, holders of public office (including members of government) and any other person involved in implementing the EU budget under shared management about the applicable provisions set out in the FR 2018 and the Public Procurement Directive with regard to the avoidance of conflicts of interest;
- Raising awareness among external partners involved in implementing the EU budget under indirect management about the applicable provisions set out in the FR 2018 with regard to the avoidance of conflicts of interest.

An own chapter provides a list of suggestions and recommendations for measures that could be put in place to avoid and manage conflict of interest situations. (TW)

Money Laundering

ECA: EU Poorly Addresses Money Laundering and Terrorist Financing

spot light

The EU's response to money laundering (ML) and terrorist financing (TF) is fragmented at the institutional level and poorly coordinated if it came to actions to prevent ML/TF and to follow-up identified risks. The EU oversight framework is insufficient to ensure a level playing field. These are the overall conclusions of the European Court of Auditors (ECA) in its Special Report 13/2021, which was released on 28 June 2021. It assesses whether the EU's actions in the area of AML/CFT are well implemented, in particular as regards the banking sector. The auditors identified a number of weaknesses on the part of the EU institutions involved in the implementation of the EU legal AML/CFT framework, i.e. the Commission, the European Banking Authority (EBA) and the European Central Bank (ECB). The weaknesses include:

- Shortcomings in drawing up the EU list of high-risk third countries whose legislation and practice are prone to ML/TF and therefore endanger the internal market – here, the work of the Commission is hindered by a lack of timely cooperation on the part of the European External Action Service; additionally, the EU has failed to establish an autonomous list that is tailored to the threats posed to the EU;
- The Commission's risk assessments for the internal market do not indicate changes over time, lack geographical focus and do not prioritise risks effectively;
- EU AML/CFT legislation is complex, transposition uneven and assessment of the transpositions by the Commission too slow (due to poor-quality communication by Member States and limited resources at the Commission);
- Although the EBA carried out thorough investigations of potential breaches of EU law, the auditors experienced lobby attempts which might have influenced EBA decision-making;
- There are no internal guidelines for triggering EBA investigations which have carried out to date on an ad hoc basis only, and, in most cases, following media reports;
- The ECB – the direct supervisor of significant euro area banks – has made a good start in sharing relevant information with national supervisors, but the information sharing is not fully efficient (*inter alia* because the ECB has neither the responsibility nor the power to investigate how such information is used at the national level);
- National supervisors use different methodologies, the quality of information provided for by the national super-

visors is varying considerably and the ECB has no specific guidance on supervisory assessments.

In conclusion, the ECA requests that the EU's supervisory role is significantly strengthened and EU law is implemented promptly and coherently. In detail, the ECA recommends that the Commission do the following:

- Prioritise ML/TF risk more clearly throughout the entire risk assessment exercise;
- Liaise with the European External Action Service for listed third countries which would ensure that intelligence is integrated in assessments;
- Make use of regulations in preference to directives where possible;
- Put in place an internal guidance for making ML/TF breach of Union law requests;
- Propose legislative amendments that clarify which information should be shared with the Commission in the breach of Union law process.

The EBA is called on to put in place rules to prevent other Board of Supervisors members from seeking to influence panel members during their deliberations. In addition, the EBA should issue guidelines that facilitate harmonised information exchanges between national and EU-level supervisors.

The ECB should put in place more efficient internal decision-making procedures and make changes to its supervisory practices once guidance from the EBA is in place.

Background: The ECA's Special Report comes during discussions to overhaul the EU's current AML/CFT framework. In May 2020, the Commission put forward a series of measures to step up the EU's AML/CFT framework (→eucrim 2/2020, 87–89). Its EU Action Plan on ML/TF already envisaged, among other things, a single EU rulebook on AML/CFT and the establishment of an EU supervisory office that would ensure a harmonised application of the AML/CFT rules. In May 2020, the Commission also tabled a refined methodology for identifying high-risk third countries. The Council adopted conclusions on the way forward as regards AML/CFT in November 2020 (→eucrim 3/2020, 177–178). ECA's conclusions and recommendations will enrich the discussions on the reform. (TW)

Tax Evasion

ECtHR Ruled in LuxLeaks Case

In a judgment of 11 May 2021, the European Court of Human Rights (ECtHR) found no violation of the freedom of expression (Art. 10 ECHR) when courts in Luxembourg convicted an insider that helped bring to light Luxembourgish tax avoidance schemes (widely known as "LuxLeaks affair"). The affair triggered several follow-up actions, including the establishment of a special committee on tax rulings in EU Member States within the European Parliament and legislative initiatives on tax transparency and whistleblower protection by the European Commission. The ECtHR acknowledged the status of whistleblower to the applicant. However, the conviction is in no disagreement with the criteria on whistleblower protection set up in ECtHR case law. The judges in Strasbourg particularly found that the Luxembourgish courts correctly balanced the public interest in receiving the information on tax rulings against the harm caused to the employer (PricewaterhouseCoopers) by the disclosures. There was also no violation of the proportionality of the penalty since the applicant was fairly modestly fined to €1000 (→judgment in *Halet v Luxembourg*, application no. 21884/18 – full text of the judgment only available in French). (TW)

Commission Initiates Public Discussion on Tax Avoidance Schemes by Shell Companies

On 4 June 2021, the Commission launched a public consultation on which action should be taken to curb the use of shell entities or legal arrangements for tax evasion purposes. The Commission points out that the EU has provided powerful instruments to tax administrations in recent years that tackle the use of abusive (often purely artificial) and aggressive tax structures by taxpayers operating cross-border in order to reduce their tax liability. However, legal entities with no or only minimal substance, performing no or very little economic activity continue to pose a risk of being used in aggressive tax planning structures. The Commission sees a need for action after investigative journalists uncovered tax-saving schemes with such legal entities in Luxembourg ("OpenLux investigation"). As a consequence, the European Parliament, journalists and civil society organisations requested clear Union rules that tackle situations involving the lack of substance of legal entities and arrangements with the purpose of minimising tax liability. The civil society has the opportunity to comment on the Commission's plans until 27 August 2021. (TW)

Practice I: VAT Scammers Caught

An action day against massive VAT fraud in mid-May 2021 resulted in the arrest of 22 suspects. The scam involved using a series of so-called front companies in different EU Member States, with suspects pretending to trade goods that, in reality, actually remained in Spain. By pretending to engage in EU trade, national VAT payment was avoided, defrauding Spanish tax authorities of €26 million in lost revenue. The operation was led by Spanish authorities and supported by authorities from the Slovak Republic, Belgium, and the Netherlands as well as by Europol and Eurojust. (CR)

Practice II: Major Hit against Fraud with Fuel Tax

At the beginning of April 2021, a large-scale operation against massive fraud with fuel taxes resulted in the arrests of 23 suspects and in the seizure of assets worth €600 million. Investigations

conducted by Italian authorities in cooperation with authorities from Bulgaria, Germany, Hungary, Malta, and Romania and supported by Eurojust helped dismantle two mafia-style organised crime groups (OCGs) from Naples and the Reggio Calabria. They had been running a fraud scheme with fuel tax worth almost €1 billion. Judicial authorities were able to make use of the new Regulation (EU) 2018/1805 on mutual recognition of freezing orders and confiscation orders, which entered into force in December 2020 (→eucrim 4/2020, 288). (CR)

Counterfeiting & Piracy

Portuguese Council Presidency Wishes to Intensify Fight against Counterfeiting

One of the priorities of the Portuguese Council Presidency in the first half of 2021 was to strengthen the criminal law protection of intellectual property rights. Against the background of growing counterfeiting and product piracy activities during the COVID-19 pandemic, the focus was laid on the connections between counterfeiting and organised crime. At the JHA Council meeting on 7 June 2021, the Presidency informed about the state of play of the discussions. All EU Member States share the view that counterfeiting and its link to organised crime is a topical matter and a major threat to public health and the economy.

The opinions differ, however, as regards the question of whether approximation of substantive criminal law to fight counterfeiting is necessary. While some Member States support common rules on criminal definitions and sanctions on the basis of Art. 83(2) TFEU, other Member States are more hesitating, arguing that first a thorough analyses on the proportionality and necessity of such measures should be carried out and the implementation of the existing framework assessed. A majority of the Ministers agreed that more efforts should be made to ensure that Member States ratified and implemented the Council of Europe Convention on counterfeiting of medical products and similar crimes involving threats to public health (MEDICRIME Convention →eucrim 2/2016, 84–85).

The Portuguese Council Presidency is of the opinion that the EU should do more besides making counterfeiting and piracy a political priority. It favours the idea of approximation of national legislation to tackle counterfeiting and its links with organised crime at least where related activities endanger the life, health and safety of individuals. The Commission is encouraged to further examine the issue of approximation. (TW)

EUIPO: Consumers Face Risks of Fake Products More than Ever

The problem of product piracy has worsened during the coronavirus pandemic, in particular due to the accompanying increase in online trade. Counterfeiters have mainly exploited people's uncertainty in the face of emerging treatments and vaccines. This is one of the key messages according to a press release issued by the EU Intellectual Property Office (EUIPO) on 8 June 2021.

The statements refer to the 2020 IP perception study, in which the EUIPO carried out over 25,000 interviews in the 27 EU Member States between 1 June and 6 July 2020 in order to assess the Europeans' perception, awareness and behaviour towards intellectual property. In addition, reference is made to a joint study carried out by the EUIPO and the OECD, which analyses the scale and magnitude of illicit trade in counterfeit pharmaceutical products, and the 2019 IP SME Scoreboard that provides insight on how small and medium-sized enterprises (SMEs) handle IP-related problems. Accordingly, the following could be observed:

- Consumers find it difficult to distinguish between genuine and fake goods;
- On average, 9% of Europeans claimed that they were mislead into buying a counterfeit product (although the proportion of mislead consumers differs among the EU Member States);
- Counterfeits represent 6.8% of EU imports, worth €121 billion;
- The proliferation of counterfeit medicines (e.g., antibiotics and painkillers) and other medical products increased in 2020;
- It is estimated that over $4 billion worth of counterfeit medicines is traded worldwide;
- Digital piracy is becoming a more and more lucrative market for infringers;
- Evidence shows that counterfeiting and privacy is closely connected with profitable activities involving organised crime groups;
- 1 of 4 SMEs in Europe claimed to have suffered from IP infringements.

Executive Director of the EUIPO, *Christian Archambeau*, said that in particular the rise of counterfeit medicines and medical products requires urgent robust, coordinated action and has recently been reinstated as one of the top ten EU priorities in the fight against organised crime. (TW)

Organised Crime

Council Sets EU's Priorities for the Fight against Organised Crime (EMPACT 2022–2025)

On 26 May 2021, based on the Europol report "SOCTA 2021" (→separate news item below), the Council adopted conclusions setting EU priorities for the period 2022–2025 to fight serious and organised crime. The conclusions fix clear goals that should be achieved within the framework of EMPACT (European Multidisciplinary Platform against Criminal Threats). Combating the following ten forms of crime is considered a priority during the next policy cycle (2022–2025):

- High-risk criminal networks (with a particular focus on those using corruption; acts of violence; firearms; and money laundering through parallel underground financial systems);

- Cyber-attacks (particularly targeting offenders who offer specialised criminal services online);
- Trafficking in human beings (with special focus on criminal networks which exploit minors, use or threaten with violence against victims and their families, and recruit and advertise victims online);
- Sexual exploitation of children;
- Smuggling of migrants (in particular as regards networks which provide facilitation services);
- Drugs trafficking;
- Fraud, economic and financial crimes (which will include the fight against online fraud schemes, excise fraud, missing trader intra community fraud (MTIC fraud), intellectual property crime, counterfeiting of goods and currencies, criminal finances and money laundering);
- Organised property crime (with a particular focus on organised burglaries, thefts and robberies, vehicle crime and illegal trade in cultural goods);
- Environmental crime (targeted here are organised crime groups with capability to infiltrate legal business structures or set up own companies to facilitate their crimes);
- Trafficking in firearms.

In addition to these priorities, the production and provision of fraudulent and false documents will be addressed as a common horizontal strategic objective.

The Council stresses the importance of the combined efforts from Member States, EU institutions, bodies and agencies, expert groups, and other stakeholders for the efficient and effective implementation of the EU's crime priorities. EMPACT is an *ad hoc* management environment to develop activities in order to achieve pre-set goals. The platform enlists the support of several EU Member States, EU institutions and agencies as well as third countries, international organisations, and other public and private partners aiming to address the main threats of organised and serious international crime. EMPACT includes both preventive and repressive measures as well as operational and strategic actions. EMPACT follows four-year cycles. The last one was adopted in 2018. In March 2021, the Council decided to continue EMPACT as a permanent instrument for cooperation to fight organised and serious international crime. (TW)

Europol's SOCTA 2021

On 12 April 2021, Europol published its Serious and Organised Crime Threat Assessment (SOCTA) for the year 2021. According to the SOCTA 2021, serious and organised crime remains a key threat to the internal security of the EU, affecting and undermining all levels of society from the daily lives of EU citizens to the economy, state institutions, and the rule of law. Criminal networks appear to have similar structures to those of business environments, including managerial layers and field operators as well as a variety of actors providing support services. One of the key characteristics of criminal networks is their ability to adapt to changes. This became apparent during the COVID-19 pandemic, with criminals quickly adapting their illegal products, modi operandi, and narratives to the unprecedented situation.

Cooperation between criminals is fluid, systematic, and driven by a profit-oriented focus. Additionally, the use of violence is increasing in terms of frequency and severity. Corruption is a feature of nearly all criminal activities in the EU, and money laundering is key to facilitating criminal profits. Furthermore, criminals control or infiltrate legal business structures in order to expedite their criminal activities. The use of modern technology is another key feature of serious and organised crime, as it helps criminals to network amongst themselves, to reach a larger number of victims, and to gain access to illegal tools and goods. The report finds that over 80% of the reported criminal networks are involved in drug trafficking, organised property crime, excise fraud, trafficking in human beings (THB), online and other forms of fraud, and migrant smuggling.

The trade in illegal drugs continues to dominate serious and organised crime in the EU in terms of the number of criminals and criminal networks involved as well as the vast amounts of criminal profits generated. While cocaine trafficking is generating multi-billion-euro profits, which are used to infiltrate and undermine the EU's economy, public institutions, and society, criminal networks are also increasing their capacities for the production and distribution of synthetic drugs. Furthermore, cyber-dependent crime has been increasing constantly in terms of both number and sophistication of attacks. This is also evident in the area of THB, where recruitment of victims and advertisement of services have moved almost entirely to the online domain. The report reports a steady increase in activities related to online child sexual abuse. The market for migrant smuggling services has remained constant. A high number of incidents in the field of organised property crime and a growing number of environmental crimes have also been observed. (CR)

Commission Presents 2021–2025 EU Strategy to Tackle Organised Crime

spot light

On 14 April 2021, the European Commission presented the new EU Strategy to tackle Organised Crime. The new strategy is part of the EU Security Union Strategy (→eucrim 2/2020, 71–73), which aims to protect European citizens from terrorism and organised crime. It also significantly draws upon Europol's 2021 report Serious and Organised Crime Threat Assessment (SOCTA →news item above).

The strategy addresses the threat that organised crime poses to European citizens, state institutions, and the economy as a whole: organised crime groups can be found across all Member States, and the business model of these groups – both online and offline – can be quite complex, as shown by the in-

vestigation that dismantled EncroChat in 2020 (→eucrim 1/2021, 22–23) The situation is exacerbated by the ability of organised groups to quickly adapt to the changing socio-economic environment. For example, some organised crime groups have been capitalising on the COVID-19 pandemic with the sale of counterfeit vaccines.

The vice-president in the *Von der Leyen* Commission with the portfolio of European Commissioner for Promoting the European Way of Life, *Margaritis Schinas*, confirmed that the strategy will help undermine the business model of organised criminal groups, which thrives on the lack of coordination between states. The new strategy is built upon the following four pillars:

(1) *Boosting law enforcement and judicial cooperation*

The Commission will:

- Expand and modernise the 2010 European Multidisciplinary Platform Against Criminal Threats (EMPACT) and establish it as the EU flagship instrument to fight organised and serious international crime. EMPACT aims to bring together all relevant European and national authorities to identify priority crime threats and address them collectively;
- Propose strengthening the 2010 Prüm framework, which allows law enforcement authorities to search for DNA, fingerprints, and vehicle registration in the databases of other Member States during their investigations;
- Propose the creation of an EU Police Cooperation Code;
- Start negotiations for agreements on cooperation between Eurojust and third countries and step up negotiations on cooperation between Europol and third countries.

(2) *Supporting more effective investigations to disrupt organised crime structures, focusing on specific serious crimes*

The Commission will:

- Revise the Environmental Crime Directive;
- Establish an EU toolbox against the counterfeiting of medical products.

Member States are urged to:

- Join and strengthen the @ON Network, which aims at improving the cooperation between law enforcement authorities, including Europol, on mafia-type organised crime groups.

(3) *Eliminating profits generated by organised crime and preventing their infiltration into the legal economy and legal businesses*

The Commission will:

- Propose a revision of the 2014 Confiscation Directive and the 2007 Council Decision on Asset Recovery Offices, in order to expand the scope of criminal offences covered;
- Assess the suitability of the existing EU anti-corruption rules countering existing criminal practices.

(4) Making law enforcement and the judiciary fit for the digital age

The Commission will:

- Identify technical and legal solutions to ensure lawful access by law enforcement authorities to encrypted information within the context of criminal investigations;
- Encourage the participation of Member States in the e-Evidence Digital Exchange System (e-EDES);
- Develop, through its Joint Research Centre, a monitoring tool to gather intelligence on illegal activities developing in the Darknet. (AP)

EMCDDA: European Drug Report 2021

On 9 June 2021, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) launched the European Drug Report 2021. The report delivers the most recent overview of the drug situation in Europe, based on data from 29 countries (27 Member States, Turkey, and Norway). Among other information, it recounts the lessons learned from the COVID-19 pandemic on how the pandemic has affected drug use and supply. It also provides a glance at Europe's drug phenomena and the latest trends in drug production and drug trafficking.

The report found, *inter alia*, that the drug market was rather resilient to the disruptions caused by the COVID-19 pandemic; criminals quickly adapted their trafficking measures and sale strategies. Levels of use of most drugs bounced back to pre-COVID-19 times when restrictions on travel, movement and social gatherings were eased in summer 2020. The report focuses on benzodiazepines on which specific concerns are raised regarding their misuse. The report lists several trends and invites politicians to discuss further reactions to new phenomena in drugs abuse and smuggling. (AP)

Eurojust: Drug Trafficking Report

On 19 April 2021, Eurojust published its Report on Drug Trafficking, reviewing experiences and identifying challenges in judicial cooperation. The report is based on an analysis of 1838 drug trafficking cases that Eurojust was involved in during the period 2017–2020. Drug trafficking remains a highly lucrative market worldwide, with an estimated value of €30 billion per year in the EU alone.

Specific issues identified by the report regarding international judicial cooperation in drug trafficking cases concern:

- New Psychoactive Substances (NPS) and their precursors;
- Cooperation with third countries;
- Controlled deliveries;
- Conflicts of jurisdiction;
- Financial investigations, asset tracing and asset recovery;
- The European Investigation Order (EIO);
- Drug trafficking in a digital environment.

Cocaine and cannabis constitute the main drug types dealt with in Eurojust's casework. According to the report, cases involving New Psychoactive Substances (NPS) and (pre-)precursors are increasingly presenting enormous legal and operational challenges for judicial authorities, due to the constant changes in substances that have not (yet) been

criminalised. Regularly updating legislation is strongly recommended to close these gaps.

Furthermore, cross-border controlled deliveries remain a sensitive issue from operational and legal points of view. Hence, the report recommends striving for greater harmonisation of and specific regulations on controlled deliveries at the EU level.

With regard to associated crimes, it appears that money laundering goes hand in hand with drug trafficking. Hence, embedded financial investigations are deemed crucial in the fight against drug trafficking, including measures for the freezing, confiscation, and recovery of assets.

Ultimately, drug trafficking in a digital environment appears to be a rapidly growing phenomenon, with more and more drug trafficking cases having links to digital marketplaces, darknet platforms, encrypted devices, etc. Therefore, judicial authorities are encouraged to seek special knowledge, for instance through the National Contact Points of the European Judicial Cybercrime Network (EJCN).

Further recommendations include making full use of existing agencies and networks such as Eurojust itself, its coordination centres, the EJN, Asset Recovery Offices (AROs), Financial Intelligence Units (FIU), and other networks. Setting up Joint Investigation Teams (JITs) should also be considered when fighting drug trafficking. (CR)

Trafficking in Human Beings

Commission to Strengthen EU Strategy on Combatting Trafficking in Human Beings

On 14 April 2021, the Commission published a Communication on the EU Strategy on Combatting Trafficking in Human Beings. By identifying key priorities and proposing concrete actions, the Commissions aims to combat trafficking in human beings more effectively. The Commission made clear that the Strategy on Combatting Trafficking in Human Beings is intertwined with the new 2021 EU Strategy to tackle Organised Crime (presented on the same day), as trafficking in human beings is often perpetrated by organised crime groups.

Regarding the new THB strategy, the Commission emphasised that it will build up on the EU Anti-trafficking Directive of 5 April 2011, which is the backbone of the EU's legislation on combatting trafficking in human beings. In so doing, the Commission intends to further support Member States in implementing the Anti-trafficking Directive. Further aims of the strategy are:

- Reducing the demand that fosters trafficking: The Commission wishes to assess the possibility of having minimum EU rules to criminalise the exploitive use of services of trafficking victims. As part of its aim to prevent human trafficking, the Commission hopes to organise awareness-raising campaigns with Member States and civil society;
- Disrupting the business model of traffickers: In an effort to disrupt the business model of traffickers, the Commission plans to enhance the coordination of law enforcement services in cross-border and international cases. This reinforcement of cooperation will be achieved by means of joint investigation teams and joint action days. In response to the relative low numbers of prosecutions and convictions of traffickers and in order to break the trafficking chain, the Commission stresses the importance of a "robust criminal justice response" based on the specific training of law enforcement and justice practitioners. With trafficking operations being increasingly conducted over the Internet, the Commission will push dialogue with the private sector and digital industries forward;
- Improving the protection of victims: This strategy seeks to protect especially women and children, as they comprise the vulnerable majority (72%) of all victims of trafficking in the EU. To protect these victims, the Commission would like to facilitate the early identification of victims by training professionals, such as border guards, police officers, social workers, and inspector services. It would also like to improve the victims' referral to further assistance and protection, especially in the cross-border context;
- Promoting closer cooperation between EU Member States, countries of origin/transit of victims and international/regional partners, including international organisations. (AP)

Cybercrime

Commission Recommends Joint Cyber Unit

On 23 June 20201, the Commission presented a recommendation on building a Joint Cyber Unit. Acccording to the Commission, the pandemic has increased the importance of connectivity and shown how important reliable and secure networks/information systems are, especially for entities in the frontline of the fight against the pandemic (e.g., hospitals and vaccine manufacturers). In order to face these challenges and prevent the loss of lives, the Commission voiced the need for a coordinated EU effort to prevent, detect, and respond to the most impactful cyber-attacks. Improved coordination between relevant cybersecurity institutions and relevant actors in the EU should also help address the cross-border nature of cybersecurity threats and the steady surge of more complex, pervasive, and targeted attacks.

Despite major progress in achieving cybersecurity – i.e., through cooperation between Member States and relevant EU institutions, bodies, and agencies (EUIs) and by means of the existing legislative framework – there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged. In addition, a mechanism does not yet exist for harnessing existing resources, providing mutual assistance

across the cyber communities, combating cybercrime, and conducting cyber-diplomacy.

In order to fill this gap and coordinate the EU effort against cyber-threats, incidents, and crises, the Commission has developed a concept for a Joint Cyber Unit that will offer coordinated assistance to Member States and EUIs in times of crisis. The platform (which will exist in both a virtual and a physical format) will involve the expertise of civilian, law enforcement, diplomatic, and cyber defence communities. The Joint Cyber Unit will identify technical and operational capabilities, experts, and equipment ready to be deployed to Member States. It is designed to provide a new impulse to European cybersecurity crisis management by ensuring a coordinated EU response. Participants in the Joint Cyber Unit should be able to engage with a wider range of stakeholders and simultaneously benefit from enhanced preparedness and greater situational awareness, covering all aspects of cybersecurity threats. Through the Unit, participants should also be able to integrate private sector stakeholders, including both providers and users of cybersecurity solutions and services.

For the purpose of establishing the Joint Cyber Unit, the Commission proposed a gradual and transparent process to be completed over the next two years. In the Annex to its Recommendation, the Commission further proposed that the objectives set out in the Recommendation be achieved in a four-step process:

- Step 1: Assessment of the Joint Cyber Unit's organisational aspects and identification of available EU operational capabilities. Step one should be fully completed by 31 December 2021.
- Step 2: Preparing Incident and Crisis Response Plans and rolling out joint preparedness activities. Step two should be fully completed by 30 June 2022.
- Step 3: Operationalising the Joint Cyber Unit. Step three should be fully completed by 31 December 2022.
- Step 4: Expanding cooperation within the Joint Cyber Unit to private entities and reporting on progress made. Step four should be fully completed by 30 June 2023. (AP)

Supporting Victims of Cybercrime

On 17 and 18 June 2021, the 10th Plenary Meeting of the European Judicial Cybercrime Network (EJCN) took place to discuss the latest trends in cybercrime and to lend support to victims of malware. The online meeting, which was hosted by Eurojust, focused on approaches to support victims of cybercrime, e.g., victim remediation. Experts also discussed how to improve investigations into large-scale online fraud schemes, which increased significantly during the COVID-19 pandemic.

The EJCN is a forum that brings together judicial practitioners specialised in countering the challenges of cybercrime, cyber-enabled crime, and investigations in cyberspace. It was established in 2016 and is hosted by Eurojust. (CR)

EU Gets Cybersecurity Competence Centre

On 20 May 2021, the Parliament adopted plans to reinforce Europe's preparedness and resilience against cyberattacks by creating a pool for innovation and expertise. In order to pool expertise in cybersecurity research and bring the European cybersecurity community of experts together, a new cybersecurity competence centre will open in Bucharest (Romania). The new legislation aims to stimulate the European cybersecurity in order to coordinate and pool relevant resources in the EU. MEP *Rasmus Andresen* sees in this new legislation a way to "ensure that all the valuable expertise that exists all across Europe – be it in research institutions, small businesses, start-ups, NGOs and the open-source community – are all included in the process of deciding European research priorities." The cybersecurity centre forms part of plans presented by the European Commission in 2017 to improve the EU's cyber resilience – the so-called "cybersecurity package" (→eucrim 3/2017, 110–111) (AP)

Europol Warning over Fake Correspondence

On 8 April 2021, Europol published a warning concerning scams with emails and messages on social media using the name of Europol's Executive Director, *Catherine de Bolle*. Europol emphasized that such correspondence is fake, especially given that its Executive Director would never directly contact members of the public requesting any immediate action or threatening to open a criminal investigation. Recipients of such scams are asked to inform Europol using a special contact form. (CR)

Terrorism

Europol TE-SAT 2021

On 22 June 2021, Europol published its EU Terrorism Situation and Trend Report (TE-SAT) 2021, which gives an overview of terrorist attacks and terrorism-related arrests in the EU in 2020. For the TE-SAT reports for previous years, →eucrim 2/2020, 95; eucrim 2/2019, 99; and eucrim 2/2018, 97. In three main chapters, the report analyses the situation regarding Jihadist, right-wing/left-wing, and anarchist terrorism.

The year 2020 saw a total of 57 completed, failed, and foiled terrorist attacks in six EU Member States, with 21 people dead and 54 people injured. In addition, 62 terrorist incidents were reported by the UK. EU Member States reported 449 individuals arrested on suspicion of terrorism-related offences in the EU in 2020. 185 arrests were reported by the UK.

According to the report, more Jihadist terrorist attacks were completed than thwarted in 2020. All 15 of the terrorist attacks – in the EU (10), Switzerland (2 probable terrorist attacks), and the UK (3) – were carried out by lone actors from diverse backgrounds, most of them using unsophisticated attack methods.

A considerable number of these perpetrators were released convicts or prisoners, which reveals the effects of Jihadist radicalisation and recruitment in prison as well as the threat stemming from released prisoners. The return of foreign terrorist fighters to Europe in 2020 was affected by COVID-19 travel restrictions with hundreds of Europeans remaining in detention camps in Northeast Syria. Furthermore, the take-down of the messenger service Telegram in 2019 had large effect to decrease Jihadist networking and operating online.

Regarding right-wing terrorism, one attack was completed by a lone actor in Germany. Three more right-wing terrorist attacks failed or were foiled in Belgium, France, and Germany. As stated in the report, suspects arrested for planning right-wing terrorist or extremist attacks are increasingly young and some are minors.

In the field of left-wing terrorism, Italy reported 24 left-wing and anarchist terrorist attacks and one attack was foiled in France. The number of arrests of left-wing extremists dropped in 2020 by more than a half compared to 2019. Europol found that left-wing and anarchists extremists addressed new topics in 2020, such as scepticism about technological and scientific developments, COVID-19 containment measures and environmental issues.

Lastly, the report lists no fundamental changes to the core terrorist *modi operandi* due to COVID-19 as terrorist groups and individuals tried to integrate the pandemic into their behaviors. (CR)

Council Conclusions: COVID-19 Impact on Terrorism and Violent Extremism

On 8 June 2021, the JHA Council adopted conclusions on the impact of the COVID-19 pandemic on terrorism and violent extremism. The conclusions follow the initiative of Portugal to assess the prevention and countering of radicalisation in the EU Member States during its Council presidency. They also contribute to the general debate in the Council as regards the consequences of COVID-19 on criminality. Looking at the current situation, the conclusions state:

- The impact of the COVID-19 pandemic on authorities responsible for countering terrorism and violent extremism has varied; security intelligence services and most law enforcement agencies were confronted with constraints on some of their activities;
- The role of the online dimension has increased since the beginning of the pandemic both as regards terrorists/extremists who shifted their activities to the Internet and authorities where online working increasingly became part of their daily life (resulting in several challenges, e.g. as to the exchange of classified information);
- Although the COVID-19 pandemic has not resulted in a clear increase in terrorist attacks, in the medium to long term, the pandemic and its socio-economic consequences might have a negative impact on terrorist and extremist threats, contributing to a growth of breeding grounds for radicalisation;
- "Coronavirus denier movements" could contribute to the potential of violence, since they attracted extremists from various ideological backgrounds.

Considering this scenario, the conclusions identified the following needs for action:

- Continuously update information that contributes to the understanding and assessment of the online dimension of the terrorist and extremist threats, particularly by providing information to the relevant EU bodies (i.e. INTCEN and Europol);
- Swiftly implement the new Regulation on the dissemination of terrorist content online;
- Continue efforts to prevent all types of illegal extremist and terrorist propaganda, the incitement of violence and the illegal financing of hate speech and violent extremism;
- Develop standard technical solutions through the EU Innovation Hub, so that the opportunities resulting from new technologies for terrorist and extremist activities can be detected and curbed;
- Enhance the development of secure channels for the exchange of classified information.

The conclusions are connected with the conclusions on the impact of COVID-19 on internal security which were also adopted at the JHA Council meeting in June 2021 (→separate news item under "Security Union"). (TW)

Environmental Crime

EP Demands Extension of EPPO Mandate to Environmental Offences

On 20 May 2021, the plenary of the European Parliament (EP) adopted, by a large majority, a resolution calling for the revision of the EU rules on the liability of companies for environmental damage. On the one hand, the Environmental Liability Directive (Directive 2004/35/EC) is to be transformed into a fully harmonising regulation applicable to all companies operating in the EU. On the other hand, the Directive on the protection of the environment through criminal law (Directive 2008/99/EC) is to be updated. Following a thorough impact assessment new types of environmental crimes should be taken into account.

MEPs also wished to ensure effective enforcement of the legislation. Prosecutor and judges should be trained accordingly. This is especially necessary since environmental crimes are estimated to be the fourth biggest type of criminal activity in the world. MEPs called on the Commission to set up an EU task force on environmental liability to help with implementation in the Member States and to provide support to victims of environmental damage.

Furthermore, MEPs called on the Commission to consider adding environmental offences as a category to the EU list of criminal offences (Art. 83(1) TFEU), so that the EP and Council can

adopt common criminal definitions and sanctions in the area of environmental protection.

MEPs deplored the low detection, investigation and conviction rates for environmental crimes. The mandate of the European Public Prosecutor's Office (EPPO), which started its operational activities on 1 June 2021, should be extended to cover environmental offences (for respective demands in literature →*Francesco de Angelis*, eucrim 4/2019, 272–276).

Ultimately, MEPs strongly condemned any forms of violence, harassment or intimidation against environmental human rights defenders and called on Member States to effectively investigate and prosecute such acts. They adopted another report urging for strong EU support and protection of environmental rights defenders and a recognition of "ecocide" as an international crime under the Rome Statute. (TW)

EU Agencies and Experts Discuss More Effectively Fighting Environmental Crime

On 6 June 2021, European Justice and Home Affairs (JHA) agencies, European Commission services, and several international organisations and expert bodies met to discuss how to fight environmental crime more effectively. The participation of different agencies and bodies enabled different perspectives to be taken on judicial aspects, the role of customs officers, maritime safety, and the links between drug trafficking and environmental crime. As part of the EU Green Deal, the seminar was one of several actions in support of the protection of the environment and the fight against environmental crime. (CR)

Global Action against Marine Pollution

On 29 April 2021, Europol released information about the results of Operation "30 Days At Sea 3.0" – a joint effort against marine pollution. The operation was conducted in March 2021 with 300 agencies across 67 countries all over the world and with the support of Europol, Frontex, and Interpol. It achieved the following results:

- Detection of 1600 marine pollution offences;
- 500 illegal acts of pollution committed at sea, including oil discharges, illegal shipbreaking, and sulphur emissions from vessels;
- 1000 pollution offences in coastal areas and in rivers, including illegal discharges of contaminants;
- 130 cases of waste trafficking through ports;
- 34,000 inspections at sea and inland waterways, coastal areas, and ports.

Next to typical forms of marine pollution crime, e.g., vessel discharges for the purpose of waste trafficking by sea, the operation also revealed the growth of new criminal trends throughout the COVID-19 pandemic, e.g., disposal of medical waste. (CR)

Racism and Xenophobia

Regulation Addressing the Dissemination of Terrorist Content Passed

spot light

After approval by the European Parliament and the Council (→eucrim 1/2021, 25), Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online was published in the Official Journal L 172 of 17 May 2021. Eucrim has informed of the negotiations of this controversial piece of legislation (last →eucrim 1/2021, 25–26; eucrim 4/2020, 284–285 with further references). The Commission tabled the proposal on 12 September 2018 (→eucrim 3/2018, 97–98). The dossier sparked fierce criticism by civil stakeholders (see also the analysis of the Commission proposal by *G. Robinson*, eucrim 4/2018, 234–240). The Regulation aims to curb the dissemination of contents by terrorists who intend to spread their messages, radicalise and recruit followers, and facilitate and direct terrorist activities.

The Regulation lays down uniform rules to address the misuse of hosting services for the dissemination to the public of terrorist content online. Particularly, it regulates the duties of care to be applied by hosting service providers (HSPs) as well as the measures to be in place on the part of Member States' authorities in order to identify and ensure the quick removal of terrorist content online and to facilitate cooperation with each other and Europol. The key elements of the new legislation are as follows:

➤ *Material scope ("terrorist content")*

- The Regulation takes up the definitions of terrorist offences set out in Directive 2017/541 on combating terrorism and makes use of them for preventive purposes. The definition of terrorist content online applies to material that:
  - Solicits someone to commit or to contribute to terrorist offences or to participate in activities of a terrorist group;
  - Incites or advocates terrorist offences, such as by glorification of terrorist acts;
  - Provides instruction on how to conduct attacks.
- Such material includes text, images, sound recordings, videos, and live transmissions of terrorist offences, which cause a danger of further such offences being committed.
- Exception: Material disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes will not be considered "terrorist content".

➤ *Personal scope*

- The Regulation applies to all hosting service providers offering services in the EU. HSPs in this sense are providers of information services which store and disseminate to the public information and material provided by users of the service on request, irrespective of whether the storing and dissemination to the public of such material is of a mere technical, automatic and passive

nature. Such platforms can be social media, video image and audio-sharing services;

■ Interpersonal communication services, such as emails or private messaging services as well as services providing cloud infrastructures do, in principle, not fall under the Regulation.

➤ *Temporal scope*

■ The obligations set out in the Regulation will apply as of 7 June 2022.

➤ *One-hour rule*

■ The Regulation considers that terrorist content is most harmful in the first hours after its appearance. Hence, HSPs will be obliged to stop the dissemination of such content as early as possible and in any event within one hour.

➤ *EU-wide removal orders*

■ The competent authority of each EU Member State has the power to issue a removal order directly requiring HSPs to remove or disable access to terrorist content in all Member States;

■ HSPs must designate or establish a contact point for the receipt of removal orders by electronic means and ensure their expeditious processing.

■ *Form and contents:* The Regulation established templates in which the authorities must fill in all the necessary information for HSPs;

■ Removal orders must contain justifications as to why the material is considered to be terrorist content, including detailed information on how to challenge the removal order.

➤ *Cross-border removal orders*

■ Where the HSP's main establishment is or its legal representative resides in a Member State other than that of the issuing authority, a copy of the removal order must be submitted simultaneously to the competent authority of that Member State;

■ The competent authority of the Member State where the HSP has its main establishment or where its legal representative resides can scrutinise the removal order issued by competent authorities of another Member State to determine whether it seriously or manifestly infringes the Regulation or the fundamental rights enshrined in the CFR;

■ Both the content provider (user) and the HSP have the right to request such scrutiny by the competent authority in the Member State where the HSP has its main establishment or where its legal representative resides;

■ The scrutiny must be carried out swiftly and a decision of whether an infringement is found must be taken within 72 hours of receiving the copy of the removal order/the request, so that it is ensured that erroneously removed or disabled content is reinstated as soon as possible;

■ Where the decision finds an infringement, the removal order will cease to have legal effects.

➤ *Proactive measures*

■ The Regulation sets out several specific measures that HSPs exposed to terrorist content online must implement to address the misuse of its services;

■ It is for the HSPs to determine which specific measures should be put in place. Such measures may include:

- Appropriate technical or operational measures or capacities, such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content;
- Mechanisms for users to report or flag alleged terrorist content;
- Any other measures the HSP considers appropriate and effective to address the availability of terrorist content on its services or to increase awareness of terrorist content;

■ HSPs are obliged to apply specific measures with effective safeguards to protect fundamental rights, in particular freedom of speech;

■ There is no obligation for HSPs to use automated tools to identify or remove content. If they choose to use such tools, they need to ensure human oversight and publicly report on their functioning.

➤ *Safeguards*

■ The Regulation installs several safeguards that are to solve conflicts with fundamental rights, in particular the freedom of speech.

■ *Transparency:* Both Member States and HSPs will be obliged to issue annual transparency reports on the measures taken and on any erroneous removals of legitimate speech online;

■ *Notification duty:* If content is removed, the user will be informed and provided with information to contest the removal;

■ *Complaints:* HSPs must establish user-friendly complaint mechanisms and ensure that complaints are dealt with expeditiously towards the content provider. The mechanisms must ensure that erroneously removed content can be reinstated as soon as possible;

■ *Legal remedies:* Content providers and HSPs must not only have the rights rights to review of the removal orders by the relevant authorities but can also seek judicial redress in courts in the respective Member States.

➤ *Sanctions*

■ Member States must adopt rules on penalties for non-compliance of the Regulation on the part of HSPs;

■ Penalties can be of an administrative or criminal nature and can take different forms (e.g. formal warnings or fines);

■ Member States must ensure that penalties imposed for the infringement of this Regulation do not encourage the removal of material which is not terrorist content;

■ In order to ensure legal certainty, the Regulation sets out which circumstances are relevant for assessing the type and level of penalties. When determining whether to impose financial penalties, due account should be taken, for instance, of the financial resources as well as the nature and size of the HSP;

■ Member States must provide that a systematic or persistent failure to comply with the "one-hour rule" following a removal order is subject to financial penalties of up to 4 % of the HSP's global turnover of the preceding business year.

The Regulation also lays down the modalities how the new rules are monitored by the Member States and evaluated by the Commission. The Commission

is requested to submit an implementation report by 7 June 2023. By 7 June 2024, the Commission shall carry out an evaluation of the Regulation and submit a report to the European Parliament and to the Council on its application.

➤ *Statements:*

Commission Vice-President *Margaritis Schinas* told journalists: "With these landmark new rules, we are cracking down on the proliferation of terrorist content online and making the EU's Security Union a reality. From now on, online platforms will have one hour to get terrorist content off the web, ensuring attacks like the one in Christchurch cannot be used to pollute screens and minds. This is a huge milestone in Europe's counter-terrorism and anti-radicalization response."

MEP *Patryk Jaki* (ECL, PL) who was the main rapporteur on the Regulation for the EP said: "I strongly believe that what we achieved is a good outcome, which balances security and freedom of speech and expression on the internet, protects legal content and access to information for every citizen in the EU, while fighting terrorism through cooperation and trust between states."

Other MEPs commented more critically. EP Vice-President *Marcel Kolaja*, who was rapporteur in the IMCO committee, criticised: "This regulation can indeed strengthen the position of authoritarians. European Pirates as well as dozens of NGOs were pointing out the issue for a long time, but most political groups ignored our warnings. We are likely to see Europe undermine its fundamental values."

Several non-governmental organisations continue to see the new Regulation as a significant threat to freedom of expression, which has not been remedied by the compromise text between the EP and the Council. In particular, the broad understanding of "terrorist content" poses the risk that orders for political purposes will be abusively issued under the guise of combating terrorism. In addition, critics predict that giving HSPs such a short deadline for removing contents would encourage them to use algorithms for their moderation, which is problematic.

It remains to be seen whether the new EU Regulation addressing the dissemination of terrorist content online can withstand a possible judicial review. (TW)

Prevention of Radicalisation in the Western Balkans

In April 2021, the European Commission agreed to continue to fund the Instrument for Pre-Accession (IPA II) with a €1.55 million project. The decision was taken to further support the Western Balkans in the prevention and countering of all forms of radicalisation. The project will enhance implementation of the Joint Action Plan on Counter-Terrorism for the Western Balkans and provide support to the Radicalisation Awareness Network (RAN), e.g., trainings, workshops, and study visits in order to improve the Western Balkans' capacity to prevent radicalisation – in line with EU policy. The project will be implemented over a period of 30 months. (CR)

Procedural Criminal Law

Procedural Safeguards

Council Conclusions on Vulnerable Persons

On 7 June 2021, the Justice and Home Affairs Council approved conclusions on the protection of vulnerable persons, with regard to civil and criminal law matters. The conclusions point out that further action is needed with regard to vulnerable adults whether they are suspects or accused in criminal proceedings or victims of crime. Vulnerable adults experience a number of difficulties, especially in cross-border situations, that may impair the full exercise of their procedural rights. The Council calls on the Member States:

- To use available funding opportunities from the EU budget to develop actions related to the protection and promotion of the rights of vulnerable adults, including on digital literacy and skills (as regards both civil and criminal law matters);
- To ensure the full implementation of the existing legislative Union framework with regard to vulnerable persons, e.g., the Victims' Rights Directive 2012/29, and share best practices on the implementation;
- To enhance the use of cross-border victims protection mechanisms within the EU, including the European protection order (Directive 2011/99);
- To ensure prompt identification of vulnerable persons and assess their vulnerability adequately in criminal proceedings (in line with the 2006 UN Convention on the Rights of Persons with Disabilities);

The Commission is invited to examine whether procedural safeguards for vulnerable adults need to be strengthened through EU law. (TW)

Data Protection

CJEU Ruled on the Powers of National Data Protection Authorities

In its ruling of 15 June 2021 in Case C-645/19, the CJEU (Grand Chamber) explained the conditions for the exercise of the powers of national supervisory authorities in cross-border processing of data. The judgment was based on the question of whether the Belgian data protection authority could take action against Facebook Belgium, although, since the entry into force of the GDPR, Facebook Ireland was the data processing entity and therefore only the Irish data protection commissioner would be authorised to bring injunctions under the control of the Irish courts. The CJEU held, that, under certain conditions, a national supervisory authority may exercise its power to bring alleged infringements of the GDPR before a court of that

Member State (here: Belgium) even if it is not the lead authority in relation to that processing.

- Conditions for the exercise of powers by a national supervisory authority which does not have the status of lead supervisory authority in relation to an instance of cross-border processing: The GDPR must confer on that supervisory authority a competence to adopt a decision finding that the data processing in question infringes the GDPR and, in addition, this power must be exercised in compliance with the cooperation and consistency procedures provided for by the GDPR.
- The exercise of the power to bring an action does not require the data controller to have a main establishment or any other establishment in the territory of the Member State.
- The power of a national supervisory authority, other than the lead supervisory authority, to initiate legal proceedings may be exercised both in relation to the main establishment and in relation to another establishment.

Ultimately, the CJEU recognises that the national supervisory authority can directly rely on the GDPR in order to bring or continue a legal action against private parties, even though the underlying obligation in the GDPR to provide this power has not been specifically implemented in the legislation of the Member State concerned. (TW)

Council Conclusions on PNR Transfers to Third Countries

At its meeting on 7–8 June 2021, the JHA Council adopted conclusions on the transfer of passenger name record (PNR) data to third countries, in particular Australia and the United States, for the purpose of combatting terrorism and serious crime. The Council emphasised that joint evaluations demonstrated the added value and operational effectiveness of the Agreements between the EU and both Australia and the United States with regard to the processing and transfer of PNR data by air carriers to the Australian and US law enforcement authorities. It also underlined that the agreements' objectives are in line with international obligations to collect, process and exchange PNR data, e.g. UN Security Council resolutions and the recent amendment to the Convention on International Civil Aviation ("Chicago Convention"). The Council, however, acknowledges that the agreements with Australia and US do not fully comply with the CJEU's Opinion 1/15 that toppled the envisaged EU-Canada PNR deal because it was not in line with the EU's Charter of Fundamental Rights and Union data protection law (→eucrim 3/2017, 114–115).

The conclusions reiterate that adequate retention is key and call on the Commission "to pursue a consistent and effective approach regarding the transfer of PNR data to third countries for the purpose of combating terrorism and serious crime, building on the ICAO SARPs [Standards and Recommended Practices on PNR of the International Civil Aviation Organization], and in line with the relevant requirements established under Union law." (TW)

Commission Adopts Sets of Standard Contractual Clauses for Safe Data Transfers

On 4 June 2021, the Commission adopted two standard contractual clauses (SCCs): one on controllers and processors in the EU/EEA and one on international transfers. With these two SCCs, the Commission is aiming to ensure safer personal data transfer by offering businesses a useful tool to ensure their compliance with the General Data Protection Regulation (GDPR) and to offer greater legal predictability to European businesses in general. These two tools take into account the CJEU's judgment *Schrems II*, in which the CJEU backed the SCC model of ensuring legal transfers of personal data to non-EU countries while clarifying the conditions for their use (→eucrim 2/2020, 98–99).

The SCCs provide companies with an easy-to-implement template, simplifying how companies verify and control their compliance with the data protection requirements. The two SCCs offer a toolbox with an overview of the different steps companies must take to comply with the *Schrems II* judgment and featuring additional examples of measures required to close existing security gaps (e.g., encryption or pseudonymisation). In order to cater to various transfer scenarios and the complexity of modern processing chains, the SCCs combine general clauses with a modular approach and offer the possibility for more than two parties to adhere to the standard contractual clauses. (AP)

EDPS Launched Two Investigations Following the "Schrems II" Judgement

On 27 May 2021, the European Data Protection Supervisor (EDPS) launched two investigations following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II") of 16 July 2020 (→eucrim 2/2020, 98–99). The two investigations, pertaining to the use of cloud services provided by Amazon Web Services and Microsoft (under Cloud II contracts by European Union institutions, bodies, and agencies (EUIs)) and the use of Microsoft Office 365 by the European Commission, are part of the EDPS' strategy for EU institutions to comply with the "Schrems II" judgement.

Following the EDPS' order to EUIs in October 2020 to report on their transfers of personal data to non-EU countries, it had been shown that individuals' personal data is being transferred outside EU and to the United States (USA), in particular. Against this background, the EDPS strongly encouraged EUIs to avoid transfers of personal data to third countries. The EDPS' analysis also showed that EUIs increasingly rely on the use of cloud computing services or platform services from large information and communications technology (ICT)

providers. Some of the ICT providers are based in the USA and therefore subject to legislation that, according to the "*Schrems II*" judgement, allows disproportionate surveillance activities to be carried out by the US authorities.

With its first investigation, the EDPS wishes to assess the EUIs' compliance with the "*Schrems II*" judgement when using cloud services provided by Amazon Web Services and Microsoft. With a second investigation, into the use of Microsoft Office 365, the EDPS would like to verify the European Commission's compliance with the recommendations issued by the EDPS, on 2 July 2020, on the use of Microsoft's products and services by EUIs. (AP)

Commission Endorses Adequacy Decision for South Korea

On 16 June 2021, the Commission initiated the procedure for adopting the adequacy decision for personal data transfers to the Republic of Korea. It will cover transfers of personal data to the Republic of Korea's commercial operators and public authorities. After having examined the legislation in the Republic of Korea, in particular the Personal Information Protection Act (PIPA) and the investigatory and enforcement powers of the Personal Information Protection Commission (PIPC), the Commission concluded that the Republic of Korea ensures a level of data protection equivalent to that guaranteed by the GDPR.

The draft adequacy decision has now been sent to the European Data Protection Board (EDPB) for its opinion. As a further step, a committee composed of representatives of the EU Member States must approve the draft before the Commission can adopt the final adequacy decision. Once adopted, data can be transmitted from the EU to South Korea without any further safeguard being necessary. In others words, transfers to the country will be assimilated to intra-EU transmissions of data. The possibility of a free flow of data would supplement the Free Trade Agreement between the EU and South Korea that entered into force in 2011. After Japan, the Republic of Korea would be the second Asian country for which the adequate protection of personal data is recognised. (TW)

EP: Commission Must Halt Adequacy Decisions that Do Not Comply with CJEU's Standards

On 20 May 2021, the European Parliament (EP) adopted a resolution on the future of data transfers to the USA following the CJEU's judgment in *Schrems II*. In this judgment (→eucrim 2/2020, 98), the CJEU found that the current legal framework allowing data transfers between the EU and the US on the basis of the "Privacy Shield" is invalid. However, it accepted the use of standard contractual clauses ("SCCs") to facilitate transfers, as long as EU-based entities verify the recipient country's level of data protection before the transfer. Suspension of data transfers may be required if the data transferred are subject to mass surveillance by US intelligence authorities.

As a reaction to the ruling in Schrems II, the EP requests, *inter alia*:

- The Commission should not conclude new adequacy decisions with third countries without taking into account the implications of EU court rulings and ensuring full GDPR compliance;
- The EDPB should give further guidance on international data transfers for companies, especially SMEs;
- Companies must continuously assess the best measures to transfer data lawfully;
- The Commission must proactively monitor the use of mass surveillance technologies in the US and in other third countries that are or could be the subject of an adequacy finding and it must not adopt adequacy decisions concerning countries where mass surveillance laws and programmes do not meet the criteria of the CJEU, either in letter or spirit;
- The Commission must bring in line current practices of exchanges of personal data with the standards set in the CJEU judgments in Schrems I and II, e.g. transfers under the Terrorist Financing Tracking Program, the EU-US PNR Agreement and agreements implementing the US Foreign Tax Compliance Act (FATCA);
- The Commission must analyse the impact of the judgments in Schrems on the EU-US Umbrella Agreement and consider consequences;
- The Union must reach digital autonomy, e.g., by investing in European data storage tools;
- The conclusion of "no-spy agreements" can be an option if the US side does not modify its surveillance laws and practice.

In general, the resolution criticises national authorities in the EU for failing to enforce the GDPR properly, as MEPs consider them to have overlooked international data transfers and failed to take meaningful corrective decisions. (TW)

Data Protection Scrutiny of Proposed Digital Green Certificate

On 21 March 2021, the European Commission published a proposal for a Regulation introducing a framework for the issuance, verification, and acceptance of interoperable certificates to citizens on vaccination, testing, and recovery to facilitate free movement during the COVID-19 pandemic. In addition, on 17 March 2021, the European Commission published a second proposal for a Regulation on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic.

On 6 April 2021, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a joint opinion on these Proposals for a Digital Green Certificate, looking at the aspects of the proposals relating to the protection of personal data. The EDPB and EDPS underline the importance of being consistent with

the General Data Protection Regulation (GDPR) and complying with the principles of necessity and proportionality. While the EDPB and EDPS acknowledge the need for a comprehensive legal framework to remove restrictions on the right to free movement, which was adopted to fight the COVID-19 pandemic, they underline the need to mitigate the (unintended) risks that may result from use of the framework, e.g., any use of personal data exceeding the intended purpose of facilitating free movement between the EU Member States.

The EDPB and EDPS recommend better defining the purpose of the Green Digital Certificate and providing a mechanism to monitor the use of the certificate by Member States. Furthermore, the proposed Regulation should expressly stipulate that access and subsequent use of the data by Member States is not permitted once the pandemic is over and define the end of the pandemic. Its scope should be limited to the current COVID-19 pandemic as well as to the purpose of facilitating the free movement of persons in the current situation. (CR)

Ne bis in idem

CJEU Judgment on Compatibility of Interpol Searches and Arrests with Ne bis in idem Principle

spot light

States that are party to the Schengen Agreement can refuse to follow an Interpol red notice seeking extradition of an individual to a third country if he/she has already been finally tried in one of the Schengen States. The CJEU delivered this groundbreaking judgment on 12 May 2021 in Case C-505/19 (*WS v Germany*).

➤ *Background of the case*

The case concerns a German citizen (*WS*) whose criminal proceedings for bribery acts were discontinued by a decision of the German prosecution office in Munich after he paid a sum of money in accordance with Sec. 153a of the German Criminal Procedure Code. He claimed that he is subject to a red notice from the USA which was distributed via the Interpol system and seeks his provisional arrest for extradition for the same offences as treated in Germany. He brought an action against the Federal Republic of Germany requesting that all necessary measures are taken in order to arrange the withdrawal of the red notice. He argued in particular that the red notice in the Interpol system infringes his right not to be prosecuted twice for the same offence as enshrined in Art. 54 CISA and Art. 50 CFR as well as his right to free movement, as guaranteed under Art. 21 TFEU. In this context, the Administrative Court of Wiesbaden referred several questions to the CJEU. A first set of questions concerned the applicability of the European ne bis in idem principle and its implications for criminal prosecution in third countries. A second set of questions related to the consequences for the processing of personal data contained in such red notices in line with the provisions of Directive (EU) 2016/680 – the EU's data protection rules for police and criminal justice authorities.

For more background information on the case, the questions referred and the opinion of AG *Bobek*, see eucrim 4/2020, 287–288 and eucrim 2/2019, 106–107.

➤ *The CJEU's findings regarding the scope of the ne bis in idem principle*

The CJEU points out that the first set of questions seek guidance of whether Art. 54 CISA and Art. 21(1) TFEU, read in the light of Art. 50 CFR, preclude the provisional arrest by the authorities of a Schengen State if the person is subject to an Interpol red notice at the request of a third State (here: USA). In the first place, the CJEU confirms its case law that Art. 54 CISA applies to procedures by which the public prosecutor of a Member State discontinues, without the involvement of a court, a prosecution brought in that State once the accused has fulfilled certain obligations, such as the payment of a sum of money set by the prosecutor (cf. judgment of 11 February 2003, Joined Cases C-187/01 and C-385/01 (*Gözütok and Brügge*)).

In the second place, the CJEU clarifies the meaning of "being prosecuted" in the sense of Art. 54 CISA, as a result of which the person concerned may not be provisionally arrested. In this context, the CJEU reiterates the objectives pursued by Art. 54 CISA, *inter alia*:

- Ensuring exercise of the freedom of movement;
- Ensuring legal certainty;
- Reflecting mutual trust in the respective criminal justice systems of the Contracting States.

However, the judges in Luxembourg stress that the European ne bis in idem principle does not bar *per se* the risk of impunity and does not preclude the maintenance of measures that prevent a person from evading justice.

In conclusion, Art. 54 CISA and Art. 21(1) TFEU preclude the provisional arrest of a person who is the subject of an Interpol red notice only if it is established by a final judicial decision that the person's trial has been finally disposed of by a State that is party to the Schengen Agreement or by an EU Member State in respect of the same acts as those forming the basis of the red notice. As soon as it is ascertained that the conditions of the ne bis in idem rule are satisfied, the authorities of the Schengen States must refrain from making a provisional arrest or keeping a person in custody following an Interpol red notice. Also these measures that are preliminary to an extradition constitute "prosecution" within the meaning of Art. 54 CISA.

The CJEU stresses that the Member States must ensure the availability of legal remedies enabling the persons concerned to obtain such final judicial decision that ascertains the applicability of the prohibition to be prosecuted twice as laid down in Art. 54 CISA.

➤ *The CJEU's findings regarding data processing*

Regarding the second set of questions, the Administrative Court of Wiesbaden

seeks to ascertain whether the authorities of the Schengen States can record and retain personal data appearing in an Interpol red notice in circumstances where the ne bis in idem principle applies. The CJEU first notes that any operation performed on those data, such as registering them in a Member State's list of wanted persons, constitutes "processing" which falls under Directive 2016/680. Such processing, however, pursues a legitimate purpose and is not unlawful solely on the ground that the ne bis in idem principle *may* apply to the acts that are described in the red notice. That processing by the authorities of the Schengen States may indeed be indispensable precisely in order to determine whether the ne bis in idem principle applies. However, the prerequisites of the data protection Directive are no longer fulfilled, i.e. record and retention of personal data are no longer necessary, if it is established that the person concerned can no longer be the subject of criminal proceedings and, consequently, cannot be arrested for the acts covered by the red notice. In this case, the data subject must be able to require erasure of his/her data. In any rate, the authorities must flag that the person concerned can no longer prosecuted in a Schengen State for the same acts by reason of the ne bis in idem principle.

➤ *Put in focus:*

The CJEU's judgment in *WS* is of extraordinary importance insofar as it grants extraterritorial effect to the European ne bis in idem principle. This guarantee as established in Art. 50 CFR and Art. 54 CISA has been thought by many scholars to have intra-Community effects only. Its scope now extends to third countries although they are not bound by Union law. The CJEU stresses that this approach is not surprising since similar effects are implied in extradition law. In accordance with the *Petruhhin* doctrine, also here EU Member States must ensure the right to move and reside freely within the territory of the EU Member States by applying the EAW system preferentially to extradition requests from third countries (→eucrim 3/2016, 131 and eucrim 4/2020, 288–289). Thus, similarities between the CJEU case law in *Petruhhin* and *WS* are evident, which the CJEU also refers to in its judgment. With regard to the scope of the ne bis in idem principle, the judges in Luxembourg fully follow the Advocate General's opinion of 19 November 2020 (→eucrim 4/2020, 287–288).

The CJEU strengthens the individual rights of citizens who have been subject to a final conviction or acquittal by the authorities of the Schengen States/EU Member States. Nevertheless, the decision is only a partial success for the prosecuted person. He must enforce a court decision in the Schengen States/EU Member States confirming the application of the transnational European ne bis in idem rule. For the time being, he is not immune from provisional arrest or other measures restricting his freedom of movement on the basis of an Interpol Red Notice. The system thus also entails that persons have to provide information on their offences in order to convince the national courts that the concluded criminal proceedings and the Red Notice cover the "same acts". This comes especially true if one considers that the description of facts and offences in red notices is regularly very brief. This burden of proof is difficult to reconcile with the principle of the presumption of innocence. In addition, in many cases, the prosecuted person will probably only successful if he organises a double defence in the countries concerned.

Ultimately, the CJEU's ruling poses major challenges especially for the legislators of the Member States. They must now create effective mechanisms, if they do not already exist, that guarantee judicial decisions on the existence of the conditions of the trans-European ne bis in idem principle. It remains to be seen whether these court decisions will resolve all individual cases without renewed involvement of the judges in Luxembourg. (TW)

EDPS Annual Report 2020

On 19 April 2021, *Wojciech Wiewiórowski,* the European Data Protection Supervisor (EDPS), presented his Annual Report 2020. It focuses on the functioning of the EDPS and the challenges if is facing during the pandemic. In the latter context, the EDPS established an internal COVID-19 task force to actively monitor and assess governmental and private sector responses to the COVID-19 pandemic. The report stressed that, despite the pandemic and even though all core activities were performed remotely, the EDPS was able to maintain a strong oversight of the EU institutions, agencies, and bodies (EUIs) as regards the processing of individuals' personal data (e.g., EDPS investigation into EUIs' use of Microsoft products and services and EDPS investigation on the European Parliament's Wi-Fi).

In order to ensure that ongoing international transfers are carried out in accordance with EU data protection law, the EDPS published its Strategy for EUIs to comply with the "Schrems II" ruling following the CJEU judgment of 16 July 2020 (→eucrim 2/2020, 98–99). In 2020, the EDPS also issued a considerable number of opinions, e.g.:

- Opinion on a proposal for temporary derogations from the ePrivacy directive for the purpose of combatting child sexual abuse online;
- Opinion on the New Pact on Migration and Asylum.

The EDPS stressed that it continued its effort to monitor technologies (such as artificial intelligence and facial recognition) in 2020 and to promote understanding about the impact of the design, deployment, and evolution of digital technology upon the fundamental rights to privacy and data protection. To strengthen cooperation between the EDPS and the EDPB, the EDPS proposed the establishment of a Support Pool of Experts (SPE) within the EDPB. The pandemic and the acceleration of digitalisation in individuals' daily lives has demonstrated the importance of an EDPS presence online in order to fully connect with the relevant target groups and stakeholders. (AP)

Victim Protection

Study Recommends anti-SLAPP Directive

In a study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI Committee, researchers from the University of Aberdeen recommended that the EU takes a legislative initiative with a view to stemming the flow of litigation which is intended to suppress public participation in matters of public interest. Europe is facing a growing phenomenon of retaliatory lawsuits that are typically brought forward by powerful actors (e.g., companies, public officials in their private capacity, high-profile persons) against persons with a watchdog function (e.g., journalists, activists, academics, trade unions, civil society organisations, etc.) in order to censor, intimidate, and silence critics – so-called "Strategic Lawsuits Against Public Participation" (SLAPPs).

The study analysed legal definitions of SLAPP and assessed the compatibility of anti-SLAPP legislation with EU law. It also looked at models of anti-SLAPP legislation in other jurisdictions (e.g. United States, Canada, Australia) and recommends that the EU should follow a distinctive approach, although good practices can be drawn from these jurisdictions. Furthermore, legislative intervention must be formulated in a manner which empowers national courts to attain the intended outcome of expeditious dismissal of cases without harming potential claimants' legitimate rights to access courts. Properly framed anti-SLAPP legislation affords the claimant the opportunity to present legitimate claims to the court and therefore satisfies the requirements of Art. 6 ECHR, the study says. It is submitted, therefore, that the relationship between the rights of pursuers and defendants in defamation cases should be revisited to remedy existing imbalance. In addition to the adoption of an anti-SLAPP EU Directive, the authors of the study recommend a recast of the Brussels Ia Regulation and a reform of the Rome II Regulation.

Since 2018, the EP has repeatedly and unsuccessfully called on the Commission in various initiatives to tackle a European regulatory proposal on SLAPP. In June 2020, civil society organisations called on the EU in a joint statement to stop gag lawsuits against public interest defenders (→eucrim 2/2020, 106–107). MEPs are making another attempt and recently submitted a draft motion for a resolution "on the strengthening democracy and media freedom and pluralism in the EU: the undue use of actions under civil and criminal law to silence journalists, NGOs and civil society". At the beginning of 2021, the EU Commission set up an expert group against SLAPP which will assist the Commission in the preparation of respective legislative proposals and policy initiatives. (TW)

Cooperation

Police Cooperation

Commission Consults Public on New EU Police Cooperation Code

The European Commission's work on a European code for cross-border police cooperation is gaining momentum. The idea was presented for the first time in the framework of the EU Security Strategy, which was presented in July 2020 (→eucrim 2/2020, 71–72). As part of the roadmap to develop a corresponding legislative proposal, citizens and stakeholders now have the opportunity to comment on the project until 14 June 2021. The aim of the initiative is to simplify and modernise cooperation between competent national authorities in the area of law enforcement. The code is to merge the various existing legislative instruments and guidelines on police cooperation into a common regulation. In addition, it is considered to include selected elements from existing bilateral agreements between Member States on police cooperation in this consolidated legal act. This could include, for example, covert investigative measures on the territory of the neighbouring state, cross-border surveillance without a judicial order in urgent cases or even custodial measures on the territory of the neighbouring state. The Commission's concrete proposal for a regulation has been announced for the fourth quarter of 2021. (TW)

Judicial Cooperation

Ministers Discuss Key Challenges for Public Prosecutors

At the JHA Council meeting on 7 June 2021, the Ministers for Justice discussed the key challenges to a well-functioning public prosecution service and how the JHA Council could engage in a more specific discussion on the topic. Discussions referred to a paper of the Portuguese Council Presidency on the "key elements for the public prosecution services including as regards judicial cooperation in criminal matters." The paper stresses the particular importance of public prosecution services for the proper functioning of the criminal justice system, effective prosecutions, and judicial cooperation in criminal matters between Member States. Ministers discussed the necessity of independence of prosecution services. They also stressed that the digitalisation of justice, adequate human and financial resources for prosecution services, and (generally) the strengthening of the resilience of justice systems are further key challenges for well-functioning public prosecution services in the EU.

The discussion on this topic was held against the background of the structured dialogue on justice-specific aspects of the rule-of-law debate. The independence and performance of public prosecution services are part of the EU's Judicial Scoreboard (→eucrim 2/2020, 74–75) and the recently introduced regular rule

of law reports from the European Commission (→eucrim 3/2020, 158–159). (TW)

Mutual Legal Assistance Agreement between EU and Japan to Be Revised

On 1 June 2021, the Commission submitted a recommendation to the Council in which it seeks authorisation to open negotiations with Japan in order to amend the EU-Japan Agreement on mutual legal assistance in criminal matters. The Agreement entered into force on 2 January 2011. It is the EU's first "self-standing" MLA agreement with a third country and includes modern cooperation tools, e.g. videoconferencing and the exchange of bank information.

The aim of the Commission's initiative is to align the MLA Agreement with the data protection rules in Directive 2016/680. It follows the Commission Communication of 24 June 2020, in which ten legal acts from the former third pillar are identified that should be aligned with the EU's new legal framework on the protection of personal data with regard to the processing by law enforcement authorities (→eucrim 2/2020, 100). The Commission proposes that the following issues should be subject to negotiations with Japan:

- Provisions on data quality and security;
- Rules on data retention and record keeping;
- Safeguards applicable to the processing of special categories of personal data;
- Restrictions on onward transfers;
- Rules on oversight and legal remedies available to individuals.

The revision of the MLA Agreement with Japan will follow the procedure of Art. 218(3) and (4) TFEU. (TW)

Report on the Impact of COVID-19 on Judicial Cooperation

On 17 May 2021, Eurojust published a report on the impact of COVID-19 on judicial cooperation in criminal matters. It was based on 128 concrete requests sent to Eurojust between April and June 2020 – when lockdowns in many countries created sudden and unexpected practical problems. The report looks at the following issues:

- The European Arrest Warrant (EAW) and extradition in relation to COVID-19;
- The impact of COVID-19 on the exchange of evidence and other investigative measures;
- COVID-19 as a criminal opportunity and corresponding asset recovery measures;
- The role of Eurojust in combating COVID-19-related crimes.

According to the report, the EAW mechanisms remained functional. However, pandemic measures had a significant effect on the final stage of EAW proceedings, i.e., the physical surrender of the requested person. Involving Eurojust seemed to have facilitated timely responses, which helped move the proceedings forward.

Member States continued to use instruments related to the exchange of evidence and to implement investigative measures. Sometimes requests were only handled in special cases, however, which led to delays in the execution of European Investigation Orders (EIOs) and requests for mutual legal assistance. Eurojust was frequently contacted to support the transmission of such orders and requests.

Understandably, pandemic measures had a strong impact on the work of Joint Investigation Teams (JITs), what with travel limitations, postponed action days, and delayed negotiations on new JITs. Eurojust quickly reacted to the situation, amending its JITs funding programme and providing JIT members with a secure communication platform on which to hold their meetings online.

In conclusion, the report calls for the establishment of reliable transmission and communication channels that practitioners can use in situations in which standard postal services are unavailable or unreliable. Hence, the report suggests establishing a single electronic platform for the exchange of the most frequently applied instruments of judicial cooperation, with access for Eurojust.

For a detailed summary of the impact of the COVID-19 pandemic on judicial cooperation and on Eurojust's role in these challenging times, see the contribution by *Ernest* and *Radu* in this issue. (CR)

European Arrest Warrant

CJEU Clarifies the Scope of the *Ne Bis in Idem* Principle Involving Sentences by Third Countries

On 29 April 2021, the CJEU, for the first time, delivered a judgment on the interpretation of Art. 4(5) of the Framework Decision on the European Arrest Warrant (FD EAW) and decided that also convictions combined with leniency measures in third countries can be a ground for refusing the execution of an EAW. The case is referred as C-665/20 PPU (*X*).

➤ *Facts of the case and questions referred*

In the case at issue, X was sought by German authorities for several criminal offences because he allegedly committed acts of exceptional violence to his partner and daughter in Berlin. X was detained in the Netherlands on the basis of the German EAW but he opposed his surrender by arguing that he has already been tried for the same acts in Iran. More specifically, he had been acquitted in respect of some of the acts and sentenced in respect of the other acts to a term of imprisonment of seven years and six months. X claimed that he served the sentence almost in full but the remainder was remitted as part of a general amnesty measure proclaimed by the Supreme Leader of the Revolution to mark the 40th anniversary of the Iranian revolution.

X invokes Art. 4(5) FD EAW, which was also transposed into Dutch law. Art. 4(5) FD EAW stipulates: "The executing judicial authority may refuse to

execute the EAW if the requested person has been finally judged by a third State in respect of the same acts provided that, where there has been sentence, the sentence has been served or is currently being served or may no longer be executed under the law of the sentencing country." This optional ground for refusal is similar to the mandatory ground for refusal in Art. 3(2) FD EAW, with the exception that the latter refers to a judgment handed down by an EU Member State, not "by a third State."

The referring Rechtbank Amsterdam has doubts whether it has a margin of discretion (although the Dutch law does not provide for one), and how it must interpret the concept of "same acts". Furthermore, the court is uncertain as regards the scope of the "enforcement condition" (i.e. "sentence has been served … or may no longer be executed…").

➤ *Findings of the CJEU*

The CJEU ruled first that – contrary to Art. 3(2) – the executing court must have a margin of discretion if it applies the refusal ground based on Art. 4(5) FD EAW. Otherwise an optional ground for refusal would turn to a genuine obligation to refuse EAWs when the person had already been tried in a third country.

Second, the CJEU clarified that the concepts in Art. 4(5), such as "same acts", must be interpreted in the same way as those in Art. 3(2) FD EAW. Therefore, the concept of "same acts" refers to the nature of the acts, encompassing a set of concrete circumstances which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected.

Third, the judges in Luxembourg stated that the enforcement condition is met in the present case. Emphasising that the wording of Art. 4(5) FD EAW refers to the "law of the sentencing country", all leniency measures provided for in the sentencing third country should be recognised if they have the effect of ceasing the imposition of the sanction. Circumstances such as the seriousness of the acts, the nature of the authority granting remission, and the matter of whether the measures are based on policy considerations, have no impact.

However, the executing court must strike a balance when exercising its discretion on the refusal ground. Therefore, the national courts must reconcile the prevention of impunity and combating crime with ensuring legal certainty towards the person concerned, including the respect of final decisions from foreign public bodies.

➤ *Put in focus*

In the first two points, the CJEU follows the opinion of Advocate General (AG) *Hogan*, which was released on 15 April 2021. The AG concluded, however, for the third question that the Iranian leniency measure is not covered by Art. 4(5) FD EAW. (TW)

AG: Amnesty Does Not Trigger *ne bis in idem* Protection

In the framework of a reference for a preliminary ruling by a Slovak court, the CJEU has to deal with the question whether the EU-wide *ne bis in idem* principle precludes the issuance of a European Arrest Warrant (EAW) when an amnesty had been granted. Advocate General (AG) *Juliane Kokott* delivered her opinion in this case (C-203/20, *AB and Others*) on 17 June 2021.

In the case at issue, the defendants are accused of having kidnapped the son of the then Slovak President in 1995 and of having committed other offences in this context. In 1998, the Slovak Prime Minister at the time issued an amnesty in this regard, which is why the criminal proceedings that had been initiated were initially discontinued. In 2017, however, the amnesty and thus also the legally binding discontinuation order were revoked by the National Council of Slovakia. On the occasion of considering the issuance of an EAW against one of the accused, the question arised whether such an EAW is compatible with the Union law prohibition of double prosecution under Art. 50 CFR (*ne bis in idem*).

AG *Kokott* examined the question of whether the discontinuance of criminal proceedings due to an amnesty is, despite the subsequent revocation of the amnesty, to be regarded as a final acquittal within the meaning of Art. 50 CFR. In this context, she noted that such a final decision must fulfil two conditions:

- It must definitively bar further prosecution;
- It must be based on a determination as to the merits of the case.

AG *Kokott* concluded that the second condition is not fulfilled if criminal proceedings are discontinued on account of amnesty. In such situations, criminal responsibility is generally not assessed.

Accordingly, the *ne bis in idem* principle under Art. 50 CFR does not preclude the issuance of an EAW where the criminal proceedings have been discontinued on account of an amnesty without an examination of the criminal responsibility of the persons concerned, but where the decision to discontinue ceased to have effect when the amnesty was revoked. (TW)

European Investigation Order

AG: Bulgaria Not Allowed to Issue EIOs

Advocate General (AG) *Michal Bobek* recommends that the CJEU decide that Bulgarian authorities cannot issue European Investigation Orders (EIOs) unless Bulgaria introduces remedies against investigative measures.

In the case at issue (C-852/19 – *Ivan Gavanozov II*), the referring Specialised Criminal Court, Bulgaria, requests clarification on whether it can request searches and seizures and a witness hearing from Czechia on the basis of an EIO, since Bulgarian law lacks any legal remedy both against the issuance of the EIO and the lawfulness of searches and seizures. The case concerns the interpretation of Art. 14(1) of Directive 2014/41 regarding the European Investigation Order (EIO Directive), which requires "Member States to ensure that legal

remedies equivalent to those available in a similar domestic case, are applicable to the investigative measures indicated in the EIO." The question is how EIOs should be handled if the national law of the issuing State does not foresee any legal remedy against (coercive) investigative measures during the investigative phase.

This question had basically already been the subject of a first preliminary ruling procedure in the given criminal proceedings against *Ivan Gavanozov* who was prosecuted in Bulgaria for large-scale VAT fraud (Case C-324/17). In contrast to the AG (→eucrim 1/2019, 36–37), the CJEU did not analyse the exact implications of Art. 14 of the EIO Directive in this case but instead confined itself to deciding on the manner in which the issuing Bulgarian authority should complete the EIO form (→eucrim 3/2019, 179).

The AG has now concluded the following:

- In accordance with the wording, context, and overarching purpose of the EIO Directive, its Art. 14(1) is applicable to legal remedies - not only in the executing but also in the issuing Member State;
- "Equivalence" within the meaning of Art. 14(1) is logically only acceptable if the situation in the issuing State is itself compatible with the minimum standards for protection of fundamental rights, as required by the CFR and the ECHR;
- In accordance with ECtHR case law, the issuing State must at least provide for (1) the possibility to challenge the legality of the search and seizure at some stage in the criminal proceedings, (2) the review and its initiation being confined to the person concerned, and (3) the review covering both the lawfulness of the measure and the manner in which it was carried out;
- If this minimum level of protection cannot be ensured by national law, the issuing Member State is not allowed to issue EIOs.

In the latter context, AG *Bobek* argues that all issued acts will, by default, be tainted because the legislation under which they were issued was itself incompatible. He refers to the ECtHR, which repeatedly found that the absence of remedies against investigative measures in Bulgaria, such as searches and seizures, is in breach of the minimum standards of Art. 13 ECHR (the right to an effective remedy). As long as the Bulgarian legislature does not remedy this situation, Bulgaria is in constant breach of fundamental rights and can therefore not take part in the mutual recognition scheme. (TW)

AG: Prosecutor Has Limited Competence to Issue EIOs

Advocate General (AG) *Manuel Campos Sánchez-Bordona* concluded that a public prosecutor is not entitled to issue a European Investigation Order (EIO) if the underlying investigative measure (here: collection of traffic and location data associated with telecommunications) can only be ordered by a court in purely domestic cases.

The case (C-724/19 – *Spetsializirana prokuratura v HP*) concerns four identical EIOs that were issued by a Bulgarian public prosecutor in the course of criminal investigations against HP and others for terrorist financing. The EIOs requested the collection of traffic and location data from electronic telecommunications in Germany, Austria, Belgium and Sweden. After execution of the EIOs, the Bulgarian criminal court, which had to examine the evidence, cast doubts on the lawfulness of the collection because traffic and location data can only be obtained on the basis of a court order in domestic cases. However, the Bulgarian law implementing Directive 2014/41 regarding the European Investigation Order (EIO Directive) simply provides that the prosecutor is the competent authority to issue EIOs in the pre-trial phase whereas the court is the competent authority in the trial phase. Thus, frictions exist with the protection of fundamental rights by the provisions in the Bulgarian Criminal Procedure Code.

According to the AG, the principle of equivalence as stipulated in Art. 6(1) lit. b) EIO Directive prohibits the issuance of an EIO by the public prosecutor if national law requires a court order for the investigative measure that is subject of the EIO. The principle of equivalence also impacts the question of competence within the meaning of Art. 2 lit. c) EIO Directive. It follows from the synopsis of both provisions that the judicial authority (judge or public prosecutor) which, within the meaning of Art. 2 lit. c) (i) EIO Directive, "is competent in the case concerned" is the one empowered under national law to order, in a purely domestic matter, the same measure that is the subject of the EIO whose adoption is at issue. The AG argues in this context that the EIO – like the European Arrest Warrant – does not allow the prosecution service to do something in cross-border cases that it is prevented from doing at the domestic level.

The case will give the CJEU the opportunity to further refine its case law on the competences of judicial authorities to issue EIOs. Recently, the CJEU decided that the German public prosecutor's office is to be considered "issuing judicial authority" in the EIO context (→eucrim 4/2020, 294).

It is also noteworthy that AG *Sánchez Bordona's* opinion comes shortly after the opinion of his colleague *Michal Bobek* who recommended in Case C-852/19 (*Ivan Gavanozov II*) that the CJEU decide that Bulgarian authorities cannot issue EIOs unless Bulgaria introduces remedies against investigative measures (previous news item). (TW)

Law Enforcement Cooperation

Organisations Reiterate their Demand for a Fundamental Rights-Based Approach to Future E-Evidence Law

European media and journalists, civil society groups, legal professional organisations and technology companies reiterated their demand that the forthcoming EU legislation on "e-evidence", which

will ease the cross-border gathering and transfer of data for use in criminal proceedings, must include strong fundamental rights safeguards. In a letter dated 18 May 2021, they regret that the negotiators in the trilogue have not fully taken into account the concerns that were previously voiced by the organisations (→eucrim 3/2020, 194; for the trilogue negotiations, →eucrim 4/2020, 295–296). They criticize, *inter alia*, the current provisions on direct cooperation between law enforcement authorities and private companies holding data that those authorities are seeking. This direct cooperation "poses serious risks of violating human rights law by undermining key fundamental rights principles, including media freedom". Key demands made by the stakeholders are:

- Greater and systematic involvement of the judicial authorities in the state where the requested data is located;
- Notification to and active confirmation by the judicial authorities in the executing state, whereby this should apply to the production of all data categories;
- Including the protection of the immunities and privileges of professionals, e.g., doctors, lawyers and journalists;
- Ensuring that production and preservation orders are subject to a prior judicial authorization or validation by a court or an independent administrative authority;
- Informing the affected person as soon as possible that the interference occurred.

It is also recommended that a secure data exchange system be set up to ensure data protection and security. (TW)

Trojan-Encrypted Device Reveals Criminal Activities

As a result of one of the largest operations against encrypted criminal activities at the beginning of June 2021, 800 suspects were arrested and over $48 million in various worldwide currencies and cryptocurrencies seized. Operation "TF Greenlight/Trojan Shield" was conducted by the US Federal Bureau of Investigation (FBI), the Dutch National Police, and the Swedish Police Authority, in cooperation with the US Drug Enforcement Administration (DEA) and 16 other countries. Europol provided support by coordinating law enforcement authorities, sharing information, and bringing intelligence into ongoing operations. By means of an encrypted device company called ANOM, run by the FBI together with its partners, messages discussing the criminal activities of over 300 criminal syndicates operating in more than 100 countries could be obtained, leading to a series of large-scale law enforcement actions being executed across 16 countries.

In 2020, law enforcement authorities, with the support of Europol, dismantled the EncroChat network that largely offered encrypted communication tools for criminals. At the beginning of 2021, Eurojust and Europol helped infiltrate Sky ECC – another service that offered encrypted communications among criminals (→eucrim 1/2021, 22–23). These police activities triggered however discussion whether the information gathered can be used as evidence in trial. On 2 July 2021, it was reported that the Regional Court of Berlin did not accept data, which was hacked in the EncroChat operation. This decision deviates from previous German Higher Regional Court decisions in other, similar cases. The difference to the ANOM operation is, however, that the police did not infiltrate a private network, but operated it itself, thus entrapping criminals who wanted to communicate undisturbed. (CR/TW)

EUROSUR Upgrade

On 9 April 2021, the European Commission adopted Implementing Regulation (EU) 2021/581, laying down additional rules for the information exchange and cooperation between EU Member States within the European Border Surveillance System (EUROSUR). New elements include easier and more secure information exchange, more effective reporting, reporting on search and rescue activities, and improved cooperation with third countries.

To better secure information exchange, the Regulation sets up an independent Security Accreditation Board composed of experts from Member States and from the Commission. It will assess the security of the relevant systems and networks in which EUROSUR data are exchanged. Furthermore, information that needs to be included in the situation reports and in the various reports has now been standardised.

In addition, the Regulation introduces monthly reports and case-to-case alerts on any situation having an impact on the EU's external borders. It also implements additional reporting obligations on incidents and operations related to search and rescue. Lastly, the Regulation contains rules for establishing and sharing specific situational reports with third countries and third parties. (CR)

Study Assesses Europol Reform Proposal

In a study for the EP's LIBE Committee, *Niovi Vavoula* and *Valsamis Mitsilegas* from Queen Mary University of London assessed the Commission's proposal on strengthening Europol's mandate (→eucrim 4/2020, 279). The study (published in May 2021) provides the EP with background information on Europol's legal framework and a legal analysis of the reform proposal, thus supporting the preparation of a forthcoming legislative report of the LIBE Committee on the revision of Europol's mandate. The study assesses the nine thematic blocks that the proposal deals with and makes several policy recommendations.

The authors stress that the reform proposal would transform the nature of the agency and its relationship to the Member States, but a proper evaluation is lacking. They submit, *inter alia*, that the planned enhanced cooperation between Europol and private parties will be a paradigm shift, which requires detailed rules on the duties of the actors. Likewise, clear definitions are necessary if Europol is enabled to process "large datasets" and carry out "digital forensics". (TW)

Council of Europe

Reported by Dr. András Csúri (AC)

Foundations

Human Rights Issues

Human Rights Commissioner: Annual Activity Report

On 21 April 2021, the Council of Europe Commissioner for Human Rights, *Dunja Mijatović*, published her 2020 annual activity report, which covers the main problems, challenges, and opportunities European countries are facing in the field of human rights. In the current global context, the Commissioner especially cautions that the COVID-19 pandemic is exacerbating long-standing problems. The activity report addresses issues that are illustrative of the negative trends currently being experienced in Europe, in particular. These issues concern public health systems, mental health care, women's rights, and the increasing pressure on human rights defenders.

The report stresses that the health crisis has aggravated long-neglected problems and inequalities in the public health system. The Commissioner therefore recommends building more inclusive and resilient health systems and making vaccines, testing, and treatment accessible to all. Mental health care also urgently needs to be reformed by accelerating the shift from institutional and coercive systems to community-based and recovery-oriented models.

In terms of women's rights, the pandemic has highlighted the persistence of violence against women and the negative impact of ultra-conservative movements on gender equality and on women's access to sexual and reproductive health care. The Commissioner therefore calls on the Member States to ratify and implement the Council of Europe Convention on preventing and combating violence against women and domestic violence ("the Istanbul Convention"). They also need to address growing online violence against women, including sexist online hate speech, which has become increasingly prevalent during the COVID-19 pandemic.

The Commissioner also voiced concern over increasing pressure on human rights defenders, in particular those working to combat Afrophobia, to protect the environment or to defend the rights of LGBTI persons. The activity report specifically highlights the serious forms of racism and racial discrimination experienced by people of African descent.

Disregard for the human rights of migrants and refugees, particularly in Italy, Greece, and the Western Balkans, is another issue of concern – one which causes thousands of avoidable deaths every year. *Mijatović* emphasised that the crisis should not justify the cessation of rescue activities and pointed to Portugal as a positive example of a country that has taken steps to ensure that all migrants have access to social, health, and other rights during an epidemic.

As regards media freedom and the safety of journalists, the Commissioner paid particular attention to freedom of expression during COVID-19 and to so-called SLAPPs (Strategic Lawsuits against Public Participation), which aim to intimidate and silence critics.

The protection and promotion of children's rights remained high on the Commissioner's agenda. The report voices serious concerns about the potential long-term adverse effects of the pandemic on children's health, safety, education, living conditions, and on the widening of existing inequalities. *Mijatović* therefore calls on Member States to ensure that the best interests of the child are paramount in all measures taken related to COVID-19.

The report also covers the Commissioner's additional activities in areas such as artificial intelligence, the independence of the judiciary and the rule of law, data protection, and the protection of the environment.

Specific Areas of Crime

Corruption

GRECO: 2020 General Activity Report

On 3 June 2021, GRECO published its 21st general activity report for the year 2020. The report finds that governments must rigorously manage the corruption risks that have arisen from the extraordinary measures needed to combat the COVID-19 epidemic, including the large influx of money into the economy to mitigate the economic and social impact of the epidemic. The report also features an article by the EU Commissioner for Justice *Didier Reynders*.

GRECO stresses that governments have had to introduce emergency measures for more than a year; they have led to concentration of powers and derogations from fundamental rights. This also entail certain risks of corruption, particularly in public procurement systems, in terms of conflicts of interest and lobbying, which should not be under-

estimated. In his introduction to the report, GRECO President *Marin Mrčela* stresses that the creation of special institutions or the adoption of new laws alone will not improve the fight against corruption, but their effective implementation will. He also calls on states to follow closely the guidelines issued by GRECO in 2020 (→eucrim 2/2020, 116–117) to prevent corruption risks in the context of the pandemic. The fight against corruption and the independence of the judiciary are interlinked and equally important, underlining that in some CoE Member States there are attempts by other branches of power to attack, intimidate or subjugate the judiciary.

The pandemic has undeniably had an impact on GRECO's work, as it was not possible to carry out any on-site visits in 2020. Nevertheless, the body adopted six evaluation reports. The annual report reviews the measures taken to prevent corruption in GRECO Member States in 2020 in the 4th evaluation round, which covers parliamentarians, judges and prosecutors, and in the 5th evaluation round, which focuses on central governments, including the highest executive functions, and law enforcement agencies. Regarding GRECO Member States' implementation efforts, the report stated that, by the end of 2020, States had fully implemented almost 40% of its recommendations to prevent corruption in respect of MPs, judges and prosecutors. The recommendations with the lowest compliance were those issued in respect of MPs (only 30% fully implemented), followed by judges (41%) and prosecutors (47%). Regarding the 5th evaluation round specifically, GRECO importantly agreed to apply a slightly different compliance procedure, which will give Member States time for in-depth reforms. The report also calls to mind that, in 2020, Kazakhstan became the 50th member state to join GRECO, with the EU now participating as an observer.

Money Laundering

PACE Resolution on Financial Intelligence Units

The Parliamentary Assembly of the Council of Europe (PACE) adopted Resolution 2365 (2021) and the accompanying Recommendation 2195 (2021), which carries the title "Urgent need to strengthen financial intelligence units – Sharper tools needed to improve confiscation of illegal assets." The documents aim to promote confiscation and AML/CFT measures and, in particular, the development of Financial Intelligence Units (FIUs).

The resolution notes that a number of different scandals, including recent leaks from the US Treasury Department's Financial Crimes Enforcement Network (FinCEN), reveal that national and international efforts to combat ML and TF have fallen far short of their intended goals. According to the World Bank, proceeds from organised crime and high-level corruption amount to trillions of US dollars annually worldwide. Only a small percentage of law enforcement agencies succeed in seizing the proceeds. The remaining amount – which accumulates in the hands of organised criminals, corrupt public officials, and terrorists – poses a huge threat to democracy, the rule of law, and national security in all Member States. At the same time, the successful confiscation of illicit assets offers a significant opportunity for states to generate the resources needed to tackle the social problems caused by organised crime, corruption, and terrorism. Urgent measures are therefore necessary to step up the tracing and confiscation of the proceeds of crime.

FIUs face the following main problems, as identified in regular national evaluations, in particular by FATF and MONEYVAL:

- Regarding reporting: uneven quality and a high volume of reports submitted by reporting entities (banks, etc.); the release of instruments by reporting entities before receiving feedback from the FIUs; lack of knowledge about the typology of ML/TF on the part of reporting entities;
- Regarding FIUs: lack of autonomy and independence of some FIUs; insufficient staff and material resources (IT equipment and tools, archiving systems); insufficient technical capacity due to new challenges (these challenges include the increasing demand for online services, Internet payment systems, and financial technology ("fintech")); the complex nature of criminal schemes; ML channels (including cybercrime);
- Regarding law enforcement: inability of law enforcement authorities to take prompt action when following up information provided by FIUs in the course of an investigation to ensure the freezing and/or seizure of assets; inability of authorities to provide timely feedback to FIUs on the quality of information disseminated and any actions taken.

Although FATF standards allow different organisational models for FIUs (administrative, law enforcement, and hybrid models), they must be given the independence, powers, and human and financial resources necessary to carry out their role effectively. The Assembly therefore calls on all CoE member states and those states having observer or co-operative status with the organisation to do the following:

- Strengthen their FIUs in accordance with the recommendations of FATF and MONEYVAL, in particular by providing them with sufficient powers, human resources, IT tools, and training facilities to enable them cope with new challenges and the increasing complexity of ML channels;
- Respect the autonomy of their countries' FIUs and refrain from political interference in their work;
- Allow FIUs to suspend suspicious transactions, both domestically and upon request of their foreign counterparts (in line with Art. 14 of the 2005 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the "Warsaw Convention"));

- Strengthen the capacity of their law enforcement agencies (police, prosecutors, and courts) by establishing specialised, well-trained, and adequately resourced working groups who cooperate closely with FIUs, so that timely actions on financial intelligence information transmitted by FIUs is taken;
- Strengthen international cooperation between FIUs by making relevant legislation and institutional structures interoperable;
- Reverse the burden of proof on the legitimacy of assets by requiring relevant persons to prove the legitimate origin of suspected assets in their possession;
- Eliminate the "citizenship for investment" schemes still being offered in some countries.

MONEYVAL: Annual Report for 2020

On 4 June 2021, MONEYVAL published its annual report for 2020. Although the pandemic has had an impact on MONEYVAL's work, the body sought to ensure continuity in the evaluation process. Last year, MONEYVAL played a pioneering role in carrying out evaluations by using virtual and hybrid tools. For the first time in the area of international AML/CFT monitoring bodies, mutual evaluation reports were adopted by virtual means (Georgia and Slovakia), and on-site visits were carried out in a hybrid format (to the Holy See and San Marino). MONEYVAL also held its first hybrid plenary meeting, with participants able to attend either physically or virtually.

The report highlights that criminals around the world have taken advantage of the pandemic situation and found new ways to abuse financial systems by committing cybercrimes, participating in fraudulent investment schemes, and selling counterfeit medicines. As reported in previous *eucrim* issues, MONEYVAL published a paper on the new threats and vulnerabilities arising from COVID-19 related crimes and their impact on ML/TF risks.

Throughout 2020, MONEYVAL was also involved in promoting the benefits of the 2005 CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the "Warsaw Convention"), in particular the possibility for FIUs to monitor and postpone suspicious transactions. The Committee of Ministers also adopted important amendments to MONEYVAL's statute, which extend its mandate to the fight against proliferation financing of weapons of mass destruction, thereby aligning it with FATF recommendations and priorities.

On average, MONEYVAL Member States and jurisdictions continued to show moderate effectiveness in their efforts to combat AML/CFT in 2020. Their average level of compliance is below the satisfactory threshold. Best results were achieved in risk assessment, international cooperation, and the use of financial information. The areas involving financial sector supervision, private sector compliance, transparency of legal entities, and ML convictions and confiscations remain particularly weak. At the end of 2020, 16 of the 19 jurisdictions evaluated by MONEYVAL in the 5th round of mutual evaluations became subject to its enhanced follow-up procedure since they had insufficiently complied with AML/TF standards.

Cooperation

Law Enforcement Cooperation

CoE Committee Adopts Draft on E-Evidence Protocol

spot light

On 28 May 2021, the CoE Cybercrime Convention Committee (T-CY), which represents the State Parties to the Budapest Convention on Cybercrime, approved the draft for the Second Protocol to the Convention. It will enhance cooperation and disclosure of electronic evidence. In parallel, the EU is discussing similar regulations following the European Commission's proposals on a more efficient cooperation to secure and obtain e-evidence within the European Union (→eucrim 1/2018, 35 and previous eucrim issues for the discussions and trilogue negotiations). The negotiations at the CoE level have also influenced the legislative dossier in the EU.

The Second Additional Protocol will, *inter alia*, lay down the conditions by means of which authorities of a State Party can directly cooperate with private entities to receive domain registration information or subscriber data. Furthermore, the following enhanced cooperation tools are provided:

- Expedited forms of cooperation between Parties for the disclosure of subscriber information and traffic data;
- Expedited cooperation and disclosure in emergency situations;
- Additional tools for mutual assistance, such as videoconferencing of experts and witnesses, and joint investigation teams.

The draft provides for several data protection and other rule of law safeguards. Parties to the Protocol may make use of reservations and declarations if required under their domestic law. For example, they may require simultaneous notification when an order is sent directly to a service provider in their territory to obtain subscriber information.

The project for drafting a second Additional Protocol to the CoE 2001 Cybercrime Convention to enhance cooperation in the field of e-evidence looks back on a long period of preparation. The first solution models have already been discussed in the CoE's working groups since 2012. In June 2017, the T-CY agreed on the Terms of Reference for the preparation of the Protocol and negotiations started in September 2017. Several rounds of consultations involving civil stakeholders were held during the negotiations. A documentation of the protocol negotiations is provided for at the T-CY Committee website. (Thomas Wahl).

Articles

Articles / Aufsätze

Fil Rouge

This issue examines a series of legal issues related to the handling of COVID-19, in particular how authorities have adapted laws and procedures to the challenges a pandemic poses. The solutions found were neither easy to implement nor always legal, as described by our various authors. The unprecedented crisis caused by the pandemic also triggered a wave of robust public investment by the Member States and the Union to save the economy, which lent itself to the accompanying risk of misuse and corruption. New measures are needed to mitigate this risk.

First, *Tartaglia Polcini's* guest editorial calls to mind that corruption is extremely flexible and easily adaptable to new scenarios, such as the COVID-19 pandemic. In times of emergency and crisis, the risk of corruption increases and has an even more debilitating effect. He stresses that the G20 played a significant role in global anti-corruption efforts and that its member countries committed to leading the international community by example and making a qualified contribution to international anti-corruption objectives and instruments.

Second, *Salazar and I* likewise address the heightened risk of corruption and other criminal phenomena that accompany the financial stimulus and economic recovery measures taken by governments in the wake of COVID-19. International organisations (United Nations, OECD) and European organisations (Council of Europe, European Union) have identified these risks, including the possible involvement of organised crime. We recommend taking timely and appropriate countermeasures ranging from prevention to prosecution. We also draw attention to the EU's new rule-of-law conditionality mechanism and argue that these measures may ultimately have a positive long-term effect on transparency and good governance.

Third, *Radu and Ernest* show that the global COVID-19 pandemic has had a far-reaching impact on the administration of public matters worldwide and generally on cooperation among states. Based on the extensive experience of Eurojust, they note that the crisis has seriously affected judicial cooperation in criminal matters. They outline, for instance, the pandemic's effect on the execution of European Arrest Warrants. There are similar impacts on other judicial cooperation measures, such as European Investigation Orders, leading to the conclusion that cooperation instruments and Eurojust itself will need to adapt to the new situation by means of digitalisation and remote but secure communication – heralding in a new digital age for judicial cooperation.

Fourth, *Fortson* describes the impact of COVID-19 on the British legal system, reiterating that several hundred pieces of legislation in which the word "coronavirus" appears in the title have been enacted since 2020. There is hardly any aspect of UK life that has not been subject to, or impacted by, coronavirus legislation, which has been largely enforced by coercive criminal sanctions. He discusses this legislation and its impact on the rule of law, on UK constitutional doctrines, on institutions, on the criminal courts, and (above all) on individuals.

Fifth, *Vavoula* critically examines the recent limitations to data protection in Greece by exploring three instances in which the authorities adapted rules and practices to COVID-19 but, in doing so, put significant pressure on protection of personal data: (1) the processing of information on individuals who obtain movement permits via SMS; (2) the tracking of COVID-19 patients; and (3) the guidelines on management of the COVID-19 crisis by the Hellenic Data Protection Authority (DPA). She argues that the Greek response to COVID-19 has been fraught with over-restrictive measures that go beyond what is necessary and proportionate in a democratic society.

Sixth, *Kappler* analyses how Germany developed legal responses to the problems of uncertainty that the new virus engendered. By giving examples, she analyses the mechanisms provided in German law to deal with these uncertainties and how the COVID-19 pandemic has posed major challenges to the law itself and to its application. Decision-making pressure was great in the face of uncertainty. She concludes, *inter alia*, that, while German law provides mechanisms enabling the legislature to act, judicial control nevertheless remains necessary.

Peter-Jozsef Csonka, Deputy Director, DG JUST of the European Commission, Member of the eucrim Editorial Board

Corruption and Bribery in the Wake of the COVID-19 Pandemic

Responses at the International and EU Levels

Peter Csonka and Lorenzo Salazar

This article describes the heightened risk of corruption and other criminal phenomena that accompany the financial stimulus and economic recovery measures taken by governments in the wake of the COVID-19 pandemic. International organisations (United Nations, OECD) and European organisations (Council of Europe, European Union) have identified these risks – including the possible involvement of organised crime – and recommended taking timely and appropriate countermeasures ranging from prevention to prosecution. The European Union has established a new conditionality mechanism for funding post-COVID-19 recovery: if a Member State does not respect the rule of law, this could undermine the principle of sound financial management, which may ultimately lead to the denial of Union funds. These measures should ideally have a positive long-term effect on transparency and good governance.

With the end to the lockdowns nearing in most Member States, we seem to be slowly overcoming the most critical period of the COVID-19 pandemic in the European Union. However, we are probably still far from having fully assessed its medium- and long-term consequences, not only in terms of human suffering – which matters most – but also in terms of legal uncertainty and economic disruption on a global scale.

This unprecedented and prolonged situation of emergency, with its destabilising effect on our social fabric and governmental structures, has created a favorable environment for criminal activities and, specifically, for corruption and bribery. Therefore, responses to this crisis from international organisations, states, and private entities should also include mechanisms for preventing, detecting, and prosecuting corruption and bribery. This is all the more urgent since governments across the world keep injecting hundreds of billions of euros to counter the negative effects of the pandemic and support investment. Recent information from media and open sources confirm the concrete risk of corrupt behaviours related to the pandemic,[1] often in relation to public procurement contracts.[2]

I. Preventing and Combating COVID-19-Related Corruption – Actions at the International Level

The international community and international and multilateral organisations/bodies engaged in the prevention of and fight against corruption, as well as leading international law enforcement institutions (e.g., Europol[3] and Interpol), civil society organisations (e.g., Transparency International[4]), and sectoral studies,[5] have clearly depicted the situation along these lines. This is why identifying and addressing corruption risks will become increasingly important in order to protect trust in public institutions and businesses, and to preserve public confidence in the ability of governments to mobilise an effective crisis response in the future. Since March 2020, all major multilateral fora have aimed to draw attention to the issue of corruption risks in the health sector, both in relation to malfeasance, in general, and to vaccines, in particular. With different emphases, these activities have attempted to identify the specific risks of corruption in the health sector and to indicate the tools and strategies to counter or at least mitigate them.

In particular, in October 2020, *Ghada Fathi Waly*, Director-General/Executive Director of the United Nations Office on Drugs and Crime (UNODC) – the world's largest agency for combating drugs trafficking, organised crime and corruption – sounded the alarm already. At the meeting of the UN countries who are party to the Palermo Convention against Transnational Organised Crime (UNTOC) in Vienna, the UN high official remarked:[6]

> "The placing of fake COVID vaccines on the online market is the most serious criminal threat today. […] Falsified COVID vaccines will soon be a lethal reality and governments need to be prepared to counter this threat."

The Secretary-General of the United Nations, *António Guterres*, made similar comments at the same event.[7] UNODC also presented a policy guidance document for the States Parties to the UN Convention Against Corruption (UNCAC) that aims at preventing corruption "in the allocation and distribution of emergency economic rescue packages in the context and aftermath of the Covid-19 pandemic."[8]

Within the Organisation for Economic Cooperation and Development (OECD), the Working Group on Bribery in International Business Transactions (WGB), the monitoring body of the 1997 OECD anti-bribery convention, underlined in Spring 2020 that some corruption risks may already be present, due to the actions put in place to mitigate the health and economic crisis generated by the pandemic.[9] Other major risks may emerge in the medium and long terms, in parallel with the full implementation of robust policies that aim to remedy the economic consequences of COVID-19. Against this background, the related risks for citizens' trust in public institutions and business are readily apparent. Another closely-related field is the counterfeiting of medical products. Noteworthy in this context is a special joint publication by the OECD and the EU Intellectual Property Office (EUIPO) that is devoted entirely to the counterfeiting of medicines.[10] In a similar vein, the Council of the European Union recently called on Member States to intensify their efforts against COVID-19-related counterfeiting and piracy, particularly given the connection of these crimes with international economic and financial crime and the involvement of organised criminal groups.[11] This stocktaking exercise may help identify existing legal differences between the Member States' criminal law frameworks, possible criminal law and prosecution gaps, and legal and practical obstacles to cross-border cooperation within the EU. The Financial Action Task Force (FATF) – the global money laundering and terrorist financing watchdog active in the OECD Headquarters – also produced a statement and a paper on the impact of the COVID-19 crisis as regards the monitoring of illicit financial flows and the combating of money laundering and terrorist financing.[12]

In light of the growing international attention paid to health sector-related corruption in the course of the pandemic, the G20 Anti-Corruption Working Group (ACWG) decided to collect national experiences in response to this threat and drew up a Compendium of Good Practices[13] offering, among other things, an overview of corruption risk hypotheses specifically related to vaccines.[14] The adoption of High Level Principles (HLP) by the ACWG is expected by the end of the Italian Presidency. The current draft provides that countries' efforts to tackle corruption in emergencies should be designed and implemented along three building blocks:

- "Preparedness", focusing on the planning and training for future events;
- "Mitigation", including measures to prevent or reduce the impact and consequences of corruption and related crimes when a crisis or emergency occurs;
- "Response and recovery", including anti-corruption measures to ensure a prompt and smooth cooperation among authorities, and a clear set of recovery rules and practices for effective restoration.

At the European level, the Council of Europe's Group of States against Corruption (GRECO) adopted guidelines on how to prevent corruption in the context of the health emergency caused by the COVID-19 pandemic.[15] The guidelines underline that the COVID-19 outbreak increases corruption risks, with the health sector being specifically exposed, in particular because of surges in the immediate need for medical supplies and the simplification of procurement rules, overcrowded medical facilities, and overburdened medical staff. While acknowledging that corrupt practices may indifferently affect the public or the private sectors, including but not limited to the procurement system, the guidelines identify bribery in medical-related services, corruption in new product research and development (including conflicts of interest and the role of lobbying), and COVID-19-specific fraud related to the marketing of counterfeit medical products as the main typologies of corruption in the health sector. GRECO stresses that transparency in the public sector is the key means of preventing corruption, whatever form it takes.

II. Protecting the EU Budget from Corruption – The EU's Conditionality Mechanism and the Role of the EPPO

As governments seek to boost post-pandemic economic recovery by investing public funds, including loans obtained through the financial markets, the need to ensure transparency and to protect these funds from corruption commensurately increases. It was in this spirit that the European Union adopted a new mechanism of conditionality[16] for the protection of its next multi-annual budget (2021–2027)[17] and its recovery funding (also known under the heading "NextGenerationEU"),[18] which together represent a massive €1,8 trillion public funding source. This new mechanism, much disputed by some governments,[19] ties Union funding to respect for the rule of law, including, *inter alia*, the requirement of effective and independent judicial authorities. Regulation 2020/2092 specifically demands that Member States have a well-working preventive and enforcement system against fraud and corruption. Recital 7 of said Regulation establishes a ground-breaking new principle:

> "Whenever Member States implement the Union budget, including resources allocated through the European Union Recovery Instrument established pursuant to Council Regulation (EU) 2020/2094, and through loans and other instruments guaranteed by the Union budget, and whatever method of implementation they use, respect for the *rule of law is an essential precondition* for compliance with the principles of *sound financial management* enshrined in Article 317 of the Treaty on the Functioning of the European Union (TFEU)."[20]

The Regulation further clarifies in Recital 8:

> "Sound financial management can only be ensured by Member States if public authorities act in accordance with the law, if cases of fraud, including tax fraud, tax evasion, corruption, conflict of inter-

> est or other breaches of the law are effectively pursued by investigative and prosecution services […]"

Art. 4 of Regulation 2020/2092 confirms that a breach of the rule of law may, *inter alia*, concern the lack of "prevention and sanctioning of fraud, including tax fraud, corruption or other breaches of Union law relating to the implementation of the Union budget or to the protection of the financial interests of the Union, and the imposition of effective and dissuasive penalties on recipients by national courts or by administrative authorities." In addition, the breach may be triggered by the lack of "effective and timely cooperation with OLAF and, subject to the participation of the Member State concerned, with the European Public Prosecutor's Office (EPPO) in their investigations or prosecutions pursuant to the applicable Union acts in accordance with the principle of sincere cooperation."

This new "conditionality" mechanism highlights the importance of the EPPO[21] in the overall system of protection of the Union's financial interests, which is required by the Lisbon Treaty[22] itself. It acknowledges the EPPO as the ultimate – and much needed – prosecution body at the EU level, responsible for overseeing and enhancing the chain of national authorities and Union agencies (i.e., OLAF, Europol, and Eurojust) active in this area. As the Union's independent prosecution body, the EPPO will undertake to investigate, prosecute, and bring to judgment cases of fraud, corruption, and other illegal activities that affect the Union's financial interests in accordance with the EPPO Regulation,[23] tackling criminal offences that are defined by national laws implementing the provisions of the "PIF Directive."[24] The core mission of this new European body is to protect EU funds from criminals in the common interest of EU citizens. Its launch on 1 June 2021 not only clearly represents a major step forward in the system of judicial protection of Union funds but also opens up a new phase in the history of European integration.

III. Concluding Remarks

In conclusion, two points appear to emerge from this brief analysis:

- The pandemic has laid bare a series of new phenomena that profoundly destabilised our economies and affected human behavior, including the ways in which people commit crime. While the urgency of stimulating the economy convinced governments to take decisive action and invest public funds in sectors that have suffered, e.g., transport, tourism, or the service industry, the availability of public funding simultaneously increased the risk of misuse, including fraud and corruption, particularly in public procurement procedures. To counter such risks, governments and international bodies have committed to enhancing control and enforcement procedures, ranging from measures ensuring transparency to better law enforcement. Examples abound that show how a crisis usually leads to long-term societal changes, and sometimes the long-term benefits may even outweigh the initial economic costs.
- A crisis is always an opportunity for governments to review their policies and adapt them to the new reality. It remains to be seen whether COVID-19 has provided such an opportunity.

1 See, *inter alia*: <https://www.ilfattoquotidiano.it/2020/11/17/covid-fiale-del-vaccino-cinese-a-roma-i-medici-sono-falsi-o-non-testati-non-vi-avventurate-nellacquisto/6006430> and <https://europa.today.it/attualita/esercito-vaccino-covid-rischio-assalti.html> and <https://www.ilfoglio.it/hacker-news/2020/05/04/news/finti-vaccini-e-test-falsificati-il-dark-web-che-lucra-sulla-pandemia-316541/> and <https://www.forzearmate.eu/2020/11/18/il-vaccino-contro-il-coronavirus-diventa-appetibile-per-le-organizzazioni-criminali-le-forze-armate-tedesche-mettono-a-disposizione-le-caserme/>. All links in this article were accessed on 21 June 2021.

2 See the experience of Eurojust (information available on the website "Eurojust and COVID-19": <https://www.eurojust.europa.eu/judicial-cooperation/tasks-and-tools-eurojust/eurojust-and-covid-19>).

3 <https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic> and <https://www.independent.co.uk/news/uk/crime/covid-vaccine-uk-latest-fake-fraud-b1722906.html>.

4 <https://www.avvisopublico.it/home/wp-content/uploads/2020/04/Transparency-Re-Act-Anticorruzione-al-tempo-del-Coronavirus.pdf>. See also the activities of other civil society organisations: <https://apps.who.int/gb/ebwha/pdf_files/WHA73/A73_R1-en.pdf>.

5 <https://it.insideover.com/societa/lombra-delle-organizzazioni-criminali-sul-vaccino-anti-covid.html> and <https://policinginsight.com/features/analysis/covid-19-criminal-acitivity-preventing-a-coronavirus-vaccine-crime-wave/>

6 <https://www.aduc.it/notizia/vaccini+falsi+anti+covid+onu+grave+minaccia_137445.php>. See also: <https://www.interris.it/news/coronavirus-vaccino/>.

7 <https://news.un.org/en/story/2020/10/1075182>.

8 United Nations Office on Drugs and Crime, "Accountability and the Prevention of Corruption in the allocation and distribution of emergency economic rescue packages in the context and aftermath of the Covid-19 pandemic", 15 April 2020 <https://www.unodc.org/documents/Advocacy-Section/COVID-19_and_Anti-Corruption-2.pdf>.

9 OECD, "Public Integrity for an Effective COVID-19 Response and Recovery", 19 April 2020, <https://www.oecd.org/coronavirus/policy-responses/public-integrity-for-an-effective-covid-19-response-and-recovery-a5c35d8c/>; OECD, "Policy measures to avoid corruption and bribery in the COVID-19 response and recovery", 26 May 2020, <https://www.oecd.org/coronavirus/policy-responses/policy-measures-to-avoid-corruption-and-bribery-in-the-covid-19-response-and-recovery-225abff3/>.

10 OECD/EUIPO, "Trade in Counterfeit Pharmaceutical Products", revised version May 2020, Paris, <https://www.oecd-ilibrary.org/governance/trade-in-counterfeit-pharmaceutical-products_a7c7e054-en>.

11 "Council conclusions on intellectual property policy (18 June 2021)", Council doc. 9932/21.

12 FATF, "COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses", May 2020, Paris, <https://www.fatf-gafi.

Peter Csonka
European Commission, Deputy Director,
Directorate Criminal Justice, DG JUST

Lorenzo Salazar
Deputy Prosecutor General to the Court
of Appeal of Naples.

org/publications/fatfgeneral/documents/covid-19-ml-tf.html>. See also the most recent World Bank intervention: <https://blogs.worldbank.org/governance/tackling-corruption-governments-covid-19-health-responses>.
13 The Compendium was published online under: <https://www.unodc.org/pdf/corruption/G20_Compendium_COVID-19_FINAL.pdf>.
14 Six national delegations (Saudi Arabia, Canada, Mexico, United Kingdom, Turkey, and Spain) have illustrated in their country responses to the Compendium the issue of vaccines, in some cases expressly indicating this sector as an area of particular vulnerability in terms of the danger of counterfeiting and unfair distribution, prices, and procurement. See pages 14, 21, 23, and 52 of the Compendium and pages 21, 40, 69, 71, 75, 138, 168, 188, 208, 209 and 212 of Annex G containing the countries' replies to the survey on corruption and COVID-19.
15 GRECO, "Corruption Risks and Useful Legal References in the context of COVID-19," 15 April 2020 <https://www.coe.int/en/web/corruption/greco-guidelines>.
16 Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget, *O.J.* L 433I, 22.12.2020, 1.
17 Council Regulation (EU, Euratom) 2020/2093 of 17 December 2020 laying down the multiannual financial framework for the period 2021 to 2027, *O.J.* L 433I, 22.12.2020, 11.
18 Council Regulation (EU) 2020/2094 of 14 December establishing a European Union Recovery Instrument to support the recovery in the aftermath of the COVID-19 crisis, *O.J.* L 433I, 22.12.2020, 23.
19 In March 2021, Hungary and Poland launched legal action at the European Court of Justice for annulment of the Regulation (Cases C-156/21 and C-157/21) – see also eucrim 1/2021, 19.
20 Emphasis added by the authors.
21 Cf. P. Csonka, A. Juszczak and E. Sason, "The Establishment of the European Public Prosecutor's Office – The Road from Vision to Reality", (2017) *eucrim,* 125–135 <https://eucrim.eu/articles/establishment-european-public-prosecutors-office/>.
22 See Art. 325(1) TFEU: "The Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through measures to be taken in accordance with this Article, which shall act as a deterrent and be such as to afford effective protection in the Member States, and in all the Union's institutions, bodies, offices and agencies."
23 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), *O.J.* L 283, 31.10.2017, 1.
24 Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, *O.J.* L 198, 28.7.2017, 29. For the Directive, see A. Juszczak and E. Sason, "The Directive on the Fight against Fraud to the Union's Financial Interests by means of Criminal Law (PFI Directive) Laying down the foundation for a better protection of the Union's financial interests?", (2017) *eucrim,* 80–87 = <https://eucrim.eu/articles/the-pfi-directive-fight-against-fraud/>.

The Impact of COVID-19 on Judicial Cooperation in Criminal Matters

The Eurojust Experience

Mariana Radu and Mário Ernest

The global COVID-19 pandemic has had a far-reaching impact on the administration of public matters worldwide and on cooperation among states in general. It has also seriously impacted judicial cooperation in criminal matters. In this note, we briefly outline the direct effect the pandemic has had on judicial cooperation in criminal matters as experienced in Eurojust casework.

From the early stages of the COVID-19 pandemic, Eurojust casework revealed that practitioners from the Member States faced a number of difficulties when dealing with cases involving judicial cooperation in criminal matters. These issues were repercussions of the measures implemented by the Member States to combat the spread of COVID-19, and they affected all instruments commonly applied in the field of judicial cooperation. The following provides a summary

of an analysis of cases registered at Eurojust since the beginning of the pandemic.[1]

Within the framework of the **European Arrest Warrant (EAW)**, Eurojust cases can be divided into three main groups, depending on which provision of the EAW Framework Decision is applied. More specifically, these cases concerned the application of Arts. 15(2), 17, and 23 of the EAW Framework Decision:

Pandemic-related measures and overall uncertainty over the functioning of judicial systems in the Member States resulted in executing authorities needing to more frequently contact issuing authorities in order to request supplementary information (Art. 15(2)). The requests made by the executing authorities most often concerned details relating to the pandemic situation in the issuing state and its impact on the surrender procedure, as well as measures applied in the issuing state regarding possible quarantine and health care available to the requested person following his/her surrender.

The cases registered with Eurojust demonstrated that the executing authorities were already aware of the obstacles existing due to the pandemic and that they sought to inform the issuing authorities about the fact that deadlines stipulated by the EAW Framework Decision would not be able to be observed (Art. 17). In several cases, the executing authorities explained that the workload of judicial authorities, in combination with the extraordinary situation, would result in failure to make a final decision on an EAW on time.

The relevant casework showed that the pandemic, particularly in its initial stages, had a serious impact on the final stage of the EAW procedure – the physical transfer of the requested person to the issuing Member State. Against the background of transfers not being possible, the issuing and executing authorities commenced negotiations, with the aim of finding a new surrender date, following the rules laid down in Art. 23 of the EAW Framework Decision. However, these negotiations were often cumbersome and exposed a lack of common EU interpretation on the applicability of Art. 23(3) – postponed surrender due to *force majeure* – and Art. 23(4) – postponed surrender on *humanitarian grounds*; another problematic issue was that a common understanding is lacking of what the relationship is between these two paragraphs of Art. 23.

Uncertainties regarding pandemic-related measures led to additional questions as to whether Art. 23 provides an appropriate legal framework for keeping the requested person in detention during these conditions and as to the application of Art. 23(5), which foresees that the requested person be released from custody within 10 days of the postponed surrender date. Despite the preliminary struggles, the EAW mechanism remained functional and, in the majority of cases, the surrender of the requested person was carried out after a new date was agreed upon.

Abrupt changes in the everyday work of judicial authorities throughout the Member States due to COVID-19 measures, including the termination of public services and limited office hours, triggered doubts regarding the feasibility of the **European Investigation Order/Mutual Legal Assistance** requests **(EIO/MLA)** execution. In the majority of these cases, the requests from practitioners concerned clarifications as to whether and how it would be possible for the executing authority to conduct witness hearings (including hearings by videoconference) or house searches. Although the execution of EIOs/MLAs was still possible, in some instances the Member States were only willing to do so in urgent and extraordinary cases.

Transmission of an EIO/MLA/**freezing order** and its follow-up were the most frequent requests for assistance addressed to Eurojust during the pandemic. The practitioners needed a reliable communication channel for a situation in which standard means or channels of communication were not available or were unreliable. From this perspective, one way forward could be the establishment of a single electronic platform to exchange the most frequently applied instruments of judicial cooperation, including access for Eurojust. This would be in line with preparations for the implementation of the e-Evidence Digital Exchange System (e-EDES), which is part of the Digital Criminal Justice project launched by the European Commission.[2] The analysed cases so far have demonstrated that practitioners can only benefit from Eurojust's access to this electronic system and thus facilitate its ability to properly fulfil its tasks.

Over the last decade, **Joint Investigation Teams (JITs)** became a frequently used judicial cooperation tool among the states. Efficient cooperation of the JIT parties requires frequent communication and regular meetings in order for them to agree on a common investigation strategy and to plan joint action days. The measures related to COVID-19 heavily affected this part of JIT cooperation and resulted in delays in planning and executing common JIT activities. The meetings of JIT members that had been scheduled in the early stages of the pandemic were cancelled or postponed for the same reason.

The pandemic also impacted the work of **Eurojust** itself. Requests to organise coordination meetings were addressed to Eurojust from the outset of the pandemic, as the national authorities needed to proceed with their investigations, discover the status of linked investigations in other states, and plan coordinated investigative actions. Despite the COVID-19 pandemic restrictions and the variety of measures implemented,

Eurojust remained fully operational. Immediately after the outbreak of the pandemic, Eurojust rapidly transitioned to remote working in order to ensure the continuation of its core business. As a result, Eurojust services, such as coordination meetings and coordination centres, were successfully held using a secure online communication platform when necessary. Specifically, in 2020, Eurojust organised 371 coordination meetings (242 by videoconference), 19 coordinated action days, and provided support to 74 newly established JITs.[3]

In addition to these activities and analyses of pandemic-related casework, Eurojust has been contributing to the Joint Eurojust–EJN compilation on the impact of COVID-19 on judicial cooperation in criminal matters.[4] This compilation combines information from the Member States in response to questionnaires launched by the Council of the European Union, Eurojust, and the European Judicial Network on pandemic-related measures having an impact on judicial cooperation. It is regularly updated and circulated among practitioners.[5]

Mariana Radu
Assistant to the National Member for Romania
Chair of the Judicial Cooperation Instruments Team Eurojust

Mário Ernest
Judicial Cooperation Advisor
Operations Department / Casework Unit
Eurojust

1 For further details, see the Eurojust Casework Report "The Impact of COVID-19 on Judicial Cooperation in Criminal Matters, May 2021, available at: <https://www.eurojust.europa.eu/impact-covid-19-judicial-cooperation-criminal-matters>. The full report is available in English. Executive summaries are also available in the other official languages of the EU.

2 For e-EDES, see Communication from the Commission, "Digitalisation of justice in the European Union – A toolbox of opportunities", COM(2020) 710 final, pp. 15, 16 (sum up at eucrim 4/2020, 262); for the Digital Criminal Justice project, see <https://www.eurojust.europa.eu/judicial-cooperation/judicial-cooperation-instruments/digital-criminal-justice>.

3 For Eurojust's work in 2020, see Eurojust, *Annual Report 2020,* March 2021, available at: <https://www.eurojust.europa.eu/eurojust-annual-report-2020-criminal-justice-across-borders-eu>. A sum up is reported at *eucrim* 1/2021, 16.

4 Cf. C. Riehle, "Eurojust/EJN: Impact of COVID-19 on Judicial Cooperation in Criminal Matters", (2020) *eucrim,* 109.

5 The updated compilations are published as a Council document (LIMITE); see the publications at the EJN website at: <https://www.ejn-crimjust.europa.eu/ejn/EJN_DynamicPage/EN/86>.

Adjusting to COVID-19 under the English Criminal Justice System

A Practitioner's Perspective

Rudi Fortson QC

From early 2020, the four nations of the United Kingdom (England, Wales, Scotland and Northern Ireland) enacted (at the time of writing) some 920 pieces of legislation in which the word "coronavirus" appears in the title. Nearly all of it is secondary legislation and much of it amends earlier versions to reflect changing conditions. There is scarcely any aspect of UK life that has not been subject to, or impacted by, coronavirus legislation that has been enforced, in large part, by coercive criminal sanctions albeit tempered by a significant degree of administrative, policing and prosecutorial discretion. This article discusses that legislation, its impact on the rule of law, on UK constitutional doctrines, on institutions, on the criminal courts, and (above all) on persons whose daily life was severely impacted by COVID-19 legislation.

I. COVID-19 and the Notion of "Law"

The general public in the UK have been on a steep learning curve as they had to assimilate legislation (that mandates compliance) together with accompanying Government 'Guidance' (that does not have the force of law *unless* a legislative measure states otherwise). Unsurprisingly, the tendency has been to conflate those sources, resulting in widespread confusion over actual legal requirements.[1]

UK coronavirus legislation has served to demonstrate that "criminalisation" is a nuanced concept, and that the notion of "lawfulness" may say as much about conduct that is permitted as it may about conduct that is prohibited. European lawyers may think the latter statement to be self-evident (applying the notion that actions are "legal" if they are expressly authorised in law). By contrast, a view, once widely held by English jurists, was that "England…is not a country where everything is forbidden except what is expressly permitted: it is a country where everything is permitted except what is expressly forbidden" (Sir *Robert Megarry* V-C).[2] This statement was cited by Lord *Sales* JSC[3] (Justice of the UK Supreme Court) who opined in *Regina v Copeland* that "[t]here is no other sensible criterion of lawfulness to be applied:"[4]

> …the general requirement that the criminal law should be clear and give fair notice to an individual of the boundaries of what he may do without attracting criminal liability supports this interpretation: "a person should not be penalised except under clear law", sometimes called the "principle against doubtful penalisation."[5]

The traditional English notion of 'lawfulness' was arguably outdated before the pandemic, but coronavirus legislation that enacted prohibitions, restrictions and permissions to regulate the actions of millions of people in the UK has challenged that notion to the limit.

II. COVID-19 Legislation and Penalising Conduct

1. Enacting COVID-19 laws

On 25 March 2020, the Coronavirus Act 2020 received Royal Assent. It enacted (among many other provisions) a power to require information relating to food supply chains (section 25); a power to suspend port operations (section 50); powers relating to potentially infectious persons (section 51); powers to issue directions relating to events, gatherings and premises (section 52); and the use of video and audio technology in criminal and civil proceedings (sections 53–57; and schedules 23–25).

However, the majority of coronavirus *regulations*, which have impacted on the movement and actions of persons, were not made under the 2020 Act, but under the 1984 Public Health (Control of Disease) Act ("PHA"). The latter was significantly amended by the Health and Social Care Act 2008, which inserted into the PHA wide-ranging "Public Health Protection" measures (sections 45A to 45T). The Government's aim was to take an 'all hazards' approach to health as reflected in the World Health Organization's International Health Regulations 2005 (which came into effect in 2007) and to address threats such as SARS[6,7]

Section 45C(1) of the PHA provides that "[t]he appropriate Minister may by regulations make provision for the purpose of preventing, protecting against, controlling or providing a public health response to the incidence or spread of infection or contamination in England and Wales (whether from risks originating there or elsewhere)". The Minister may impose or enable the imposition of "restrictions or requirements on or in relation to persons, things or premises in the event of, or in response to, a threat to public health" (s. 45C(3)). Section 45F(2) stipulates that regulations may (among other things), (a) confer functions on local authorities and other persons; (b) create offences; (c) enable a court to order a person convicted of any such offence to take or pay for remedial action in appropriate circumstances; and (d) enact statutory measures for the execution and enforcement of restrictions and requirements imposed by or under the regulations.

Such regulations must be laid before Parliament but this is subject to an "emergency procedure" by which an instrument containing health protection measures may be made provided that it declares that "the person making it is of the opinion that, by reason of urgency, it is necessary to make the order without a draft being [laid before Parliament] and approved" (s.45R(2)). A number of COVID-19 regulations have been made in this way and brought into force. Shortly thereafter, they were laid before Parliament (and presumably approved).[8] Measures that are introduced on the basis of a state of emergency challenge fundamental legal and constitutional principles.[9] Certain COVID-19 regulations required (among other things) specified premises and business to close or to provide a restricted service; and/or mandated that "no person may leave the place where they are living without reasonable excuse"[10] (subject to certain exceptions); and/or that "no person may participate in a gathering in a public place of more than [x] people" (save in specified circumstances).[11]

2. Criminalisation and penalisation

By section 45F(5) PHA, "health protection regulations" may not create an offence triable on indictment (that is to say, triable in a Crown Court) or punishable with imprisonment. However, the regulations could – and did – create 'summary

offences' (that is to say, triable in a Magistrates' Court) punishable by way of a fine or a "fixed penalty notice". The aim of the latter was clearly intended to avoid giving offenders a criminal record for one or more breaches of the regulations, but this required police officers to correctly identify an actual breach – and this they could only do if the law was clear and if penalisation was not doubtful.

In practice, penalisation often occupied grey areas of the coronavirus regulations. Thus, when regulations specified that persons (and groups of persons) were not permitted to "mingle",[12] it was left to individuals and to the police to work out in their minds what this expression meant.[13] Insofar as the regulations prohibited certain conduct in the absence of a "reasonable excuse" (e.g., leaving home or travelling outside the UK, or failing to comply with a restriction[14]) the limits of that defence were illustrated (to some extent) by situations, particularised in the regulations, each of which constituted a "reasonable excuse". However, much was left to personal judgment.[15]

Although a statutory defence of "reasonable excuse" might be thought to offend the 'principle against doubtful penalisation', it is available under English law in respect of many statutory offences.[16] In some contexts (such as restricting the right of persons to gather to protest) the defence of "reasonable excuse" may be the means by which the legislation in question satisfies Arts. 10 and 11 of the ECHR (and Arts. 10 and 11 of the UK Human Rights Act 1998) – the rights to freedom of expression and to freedom of assembly/association.[17]

Occasionally, one open-textured expression in a regulation was linked with another, thereby compounding problems of interpretation and comprehension. For example, there had been a statutory requirement on persons (in specified areas of England) not to "leave or be outside of the place where they are living without reasonable excuse"[18] save when "reasonably necessary…to take exercise outside".[19] Although Government guidance stated that "exercise" "should be limited to once per day, and you should not travel outside your local area", this was not incorporated within the regulations (and thus the guidance lacked the force of law) and there was no legal definition of "local area".[20] Two women, who were fined £200 each when they drove five miles for a walk, had their fixed penalties withdrawn.[21] In those circumstances, and given the actual law that applied, the final outcome was inevitable.

3. Public confidence in the law and law enforcement

A defence of "reasonable excuse" usually gives rise to few problems in practice (e.g. legislation relating to offensive weapons and firearms). This may be because few persons have offensive weapons with them in public places and thus, making a judgment on the merits of a given case, is relatively straightforward. By contrast, the COVID-19 legislation imposed obligations on millions of people to desist from doing much that they would normally do (or even be expected to do).[22] Accordingly, those who construed the 'rules' restrictively were often ready to accuse others of 'breaking' them when, in fact, the legal position was unclear. Sometimes public reaction to a perceived breach, 'boiled over'. At a time when national travelling restrictions were in place, it was reported that the Prime Minister's then Chief Adviser (*Dominic Cummings*) travelled from London to Durham having gone to work at Downing Street (after his wife became ill with COVID-19 symptoms) rather than isolating at home for 14 days. It was reported further that, whilst staying away from his home in London, the Adviser made a journey to Barnard Castle. The Director of Public Prosecutions (DPP) decided not to refer the case to the police for investigation of a potential breach the regulations[23] and/or a potential offence of public nuisance, contrary to common law. A member of the public unsuccessfully sought the permission of the Administrative Court to challenge that decision by way of judicial review (R (on the application of) Redston v DPP[24]). The judgment focused on the question of whether or not the DPP had power to refer (or even to 'nudge') a case to the police for investigation. The Court concluded that the DPP had no such power because "such power or discretion would run counter to the distinction between investigative responsibility and prosecutorial responsibility which is so clearly expressed in the [Prosecution of Offences Act 1985]". The Court considered that even a 'nudge' would represent "an impermissible trespass over the investigation/prosecution boundary" (per Lady Justice Carr DBE).

4. Miscarriages of justice

In May 2021, the Crown Prosecution Service published its 'review findings' for prosecutions under the Coronavirus Act 2020 and the Health Protection Regulations between 26 March 2020 and 31 March 2021.[25] Of 1,821 finalised cases, 549 cases were identified by prosecutors as having been incorrectly charged and these were either withdrawn or set aside. Most cases (1,551) were brought under the Regulations. The majority of those cases (82%: 1,272) had been correctly charged. Of the 270 cases charged under the Coronavirus Act 2020, all had been incorrectly charged and thus failed. The UK Parliamentary Joint Committee on Human Rights remarked that:

> It is astonishing that the Coronavirus Act is still being misunderstood and wrongly applied by police to such an extent that every single criminal charge brought under the Act has been brought incorrectly. While the coronavirus Regulations have changed frequently, the Act has not, and there is no reason for such mistakes to continue.[26]

III. The Impact of COVID-19 on Traditional UK Doctrines and Processes – the Example of Open Justice

Some COVID-19 restrictions threatened to compromise certain well-established doctrines, practices and processes that are the essence of the UK constitution. Many aspects of UK democracy are enshrined in law and they may also be supported or circumscribed by the criminal law. Quite apart from legal rules pertaining to freedom of expression[27] and the right to protest, there are (for example) rules that oblige certain meetings to be held (for example, certain company meetings).[28]

The criminal courts operate under the principle of 'open justice'. Except in rare situations, criminal proceedings are conducted in open court. Typically, all the participants will be physically present in the courtroom. Members of the public and the press may occupy a dedicated part of the courtroom to observe the proceedings. Ensuring that proceedings are compliant with the ECHR/the Human Rights Act 1998[29] is of paramount importance. Accordingly, the Coronavirus Act 2020 made extensive provision for conducting criminal proceedings in ways that would respect public health whilst maintaining the traditional concepts of open justice and due process. As a recent report stressed:

> [Fairness] in criminal proceedings can be undermined if new technologies are deployed in ways that do not take into account the specific needs of the defence in the digital era.[30]

Some statutory COVID-19 measures (see, for example, 1 and 2 below) have extended or modified pre-existing procedures for conducting criminal proceedings whilst 'achieving best evidence'[31] in those proceedings.

1. Live audio and live video links

Provisions enacted under the Criminal Justice Act (CJA) 2003 (for example, the provision of "live links"[32] in criminal proceedings: section 51) were modified so that a person (other than a member of a jury[33]) "may, if the court so directs, take part in eligible criminal proceedings through (a) a live audio link, or (b) a live video link".[34] Such proceedings included a summary trial or a trial on indictment, and an appeal to the Court of Appeal (Criminal Division).[35] A "live audio link" meant a "live telephone link or other arrangement" which enabled a participant to hear and to be heard by every other person "taking part in the proceedings who are not in the same location".[36] Similarly, a "live video link" meant "a live television link or other arrangement" which enabled a participant and "all other persons taking part in the proceedings" to see and hear that person.[37] The court could not give an audio/video live-link direction unless the court was satisfied that it was "in the interests of justice" for the person concerned to take part in the proceedings in that way and the parties to the proceedings had been given the opportunity to make representations.[38] Where the defendant was under 18 years of age (or the court decided to continue to deal with the case as if the defendant had not attained that age) the "youth offending team" had to be given the opportunity to make representations before proceeding by way of a live link.[39]

A live-link direction could only be given once the court had considered "all the circumstances of the case"[40] including (but not limited to) the factors set out in modified s. 51(7), CJA 2003.[41] Section 51(4B) and schd. 3A, CJA 2003, placed some limitations and prohibitions on the use of live links.[42] When evidence was given by live link, it was open to the judge to give the jury (if there was one) "such direction as he thinks necessary to ensure that the jury gives the same weight to the evidence as if it had been given by the witness in the courtroom or other place where the proceedings are held."[43]

Powers under the Crime and Disorder Act 1998 were also modified by the Coronavirus Act 2020[44] to encompass preliminary hearings, sentencing and enforcement hearings[45] so that such hearings could be conducted by way of an audio or video live link if it was in the interests of justice to do so.[46]

2. Conducting and managing remote hearings

As a result of the statutory modifications mentioned above, remote court hearings emerged in two forms. The first was an all-virtual hearing, and the second was a hybrid hearing. Different judges adopted slightly different practices. Some judges were located away from a court centre when conducting (for example) a preliminary hearing, but other judges attended the centre in person. As for the former, it must be remembered that some judges were especially vulnerable to contracting COVID-19 and thus they required a degree of 'shielding'. The hybrid version involved key participants attending court premises (typically, defendants, advocates, judges, and jurors (if any)) but evidence might be given by live link. In some cases, the advocates were required to 'self-isolate' (having tested positive for COVID-19) but they were able to participate via a live link.

Conducting contested trials on indictment (with a jury) under strict COVID-19 conditions ('lockdown') was often a challenging experience, especially in cases involving two or more defendants charged jointly. Courts (and their equipment) were not designed with a pandemic in mind. Participants had to be kept 'socially distanced' from each other, and this included the lawyers, jurors, and defendants. Some court 'docks' were not of sufficient size to seat two or more defendants in a 'socially

distanced' way (e.g. 2 metres apart) and thus a trial might require two courts to conduct it. Each court had to be equipped with audio and video live links to ensure that each participant was in sight and hearing of each other (except where a witness had been granted 'special measures' that entitled him or her to give evidence out of sight of one or more persons or class of persons). The two courts had to be in communication with each other and be in a position to receive and to transmit video and audio data to other locations (e.g. where a witness was located).

Static cameras in a courtroom, which were designed to focus on (e.g. the judge), might not capture a 'head-and-shoulders' image of a witness or to stream an image of the dock in the neighbouring court. In an English criminal trial, the demeanour of persons (especially witnesses) is regarded – mistakenly or otherwise[47] – as a matter of considerable importance.

The use of live-link technology in court proceedings requires a stable and reliable connection that may be required to stream data for many hours. Sound and video quality is obviously important. But the live streaming and broadcasting of data must also be secure and free from interception or other misuse. Even before the pandemic, data 'platforms' (approved by the Ministry of Justice) were in existence (and updated) to achieve and to maintain data protection standards as well as traditional procedural requirements (for example, the unauthorised photographing or audio recording of criminal proceedings).

It has been pointed out (fairly) by *Sorabji* and *Vaughan* that "the senior judiciary relied predominately on soft law in the form of judicial guidance and protocols to manage the system"[48] (that is to say, the criminal justice system) with the aim of maintaining individual and public health whilst endeavouring to proceed with court business in accordance with substantive and procedural law).[49] Similarly, local court centres took steps to manage their premises and caseload, and they adjusted certain in-court practices to promote the health and wellbeing of court users.

However, slip-ups (hopefully exceedingly rare) did occur. In the civil case of *Gubarev and Anor v Orbis Business Intelligence Ltd and Anor*,[50] a 'Zoom' link to the live streaming of court proceedings had mistakenly been provided to (among others) certain persons connected with the claimants. The observations of Dame *Victoria Sharp* P (giving the judgment of the court) powerfully illustrate some of the difficulties confronting judges and practitioners when a hybrid hearing is being conducted:

> 50. …whether a court hearing is a remote hearing or a hybrid hearing…or a conventional face to face hearing, it must be conducted in a way that is as close as possible to the pre-pandemic norm.
>
> 51. In normal circumstances a judge can see and hear everything that is going on in court. The judge can see who is present, and whether a witness who is giving live evidence has been present in court observing and listening to the evidence of other witnesses. The judge can see whether someone is attempting to influence, coach or intimidate a witness whilst they are giving evidence. The judge can immediately see…that a person sitting in court who is not a journalist appears to be tweeting on their mobile phone without first obtaining permission. That a judge can see and hear everything that happens in court enables the judge to maintain order, discipline and control over what is done in court, and thus to maintain the dignity and the integrity of the proceedings as a whole. This control extends to the recording of images and sounds of what goes on in court and what is then used outside court.
>
> 52. Once live streaming or any other form of live transmission takes place, however, the Court's ability to maintain control is substantially diminished, in particular where information is disseminated outside the jurisdiction, as happened in this case. The opportunity for misuse (via social media for example) is correspondingly enhanced, with the risk that public trust and confidence in the judiciary and in the justice system will be undermined. In these circumstances, it is critical that those who have the conduct of proceedings should understand the legal framework within which those proceedings are conducted, and that the Court is able to trust legal representatives to take the necessary steps to ensure that the orders made by the Courts are obeyed.

IV. The Future

There is no doubt that much has been learned by policy makers and by legal practitioners from the COVID-19 experience in the conduct of criminal proceedings. Case management hearings and uncontentious matters are ideally suited to virtual/remote hearings. However, receiving and giving evidence remotely has significant drawbacks – especially if the technology does not replicate (as close as possible) the experience of giving evidence in the normal way. Interrupted transmission, poor sound quality, or delays in transmission (between question and answer) and poor video quality, are not conducive (it is submitted) to receiving the best evidence. Gestures and facial expressions made by a witness over a video link (especially in close-up) may or may not be distracting, and those expressions may or may not be meaningful of the reliability and credibility of that witness' testimony. Further research into evidence that is given by live link is arguably warranted. The COVID-19 experience also reinforces the correctness of Sir *Robert Megarry's* statement that the criminal law "should be clear and give fair notice to an individual of the boundaries of what he may do without attracting criminal liability".

1 For example, when 'lockdown' eased on the 17th May 2021 (under "step 3" of the UK Government's "roadmap"), politicians and commentators opined whether it would be permissible for persons to "hug" each other and perhaps to "shake hands". In fact, the *regulations* never expressly forbade the shaking of hands or even hugging within permitted groups of persons.

Rudi Fortson QC
Barrister, 25 Bedford Row, London; Visiting Professor of Law, Queen Mary University of London

2 *Malone v Metropolitan Police Comr* [1979] Ch 344, at 357.
3 In support of a majority decision of the UK Supreme Court in *R v Copeland* [2020] UKSC 8.
4 *R v Copeland* [2020] UKSC 8, at [28].
5 Citing Bennion, *Statutory Interpretation*, 7th ed. 2017, section 27.1.
6 Severe Acute Respiratory Syndrome.
7 See the Explanatory Notes to the Health and Social Care Act 2008.
8 See on the application of *Dolan and others* [2020] EWCA Civ 1605, at [86].
9 For invaluable discussions on this topic, see V. Mitsilegas, 'Responding to Covid-19: Surveillance, Trust and the Rule of Law', *Responding to Covid-19 blog* (Queen Mary University of London – Criminal Justice Centre), 26 May 2020, <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/responding-to-covid-19-surveillance-trust-and-the-rule-of-law.html>; E. Guild, 'EU Fundamental Rights, Human Rights and Free Movement in times of Covid19', *Responding to Covid-19 blog* (Queen Mary University of London - Criminal Justice Centre), 24 July 2020, <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/eu-fundamental-rights-human-rights-and-free-movement-in-times-of-covid19.html>. All hyperlinks in this article were last accessed on 1 July 2021.
10 For example, SI 2020 No. 350.
11 For example, SI 2020 No. 350.
12 For example, SI 2020, No. 986.
13 See R. Fortson, 'Mingling and the Rule of Six', *Responding to Covid-19 blog* (Queen Mary University of London – Criminal Justice Centre), 16 September 2020, <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/mingling-and-the-rule-of-six.html>.
14 For example, SI 2020 No. 1374.
15 See R. Fortson, 'Open textured legislation in the times of Covid-19: 'reasonable excuse' and legal certainty', Responding to Covid-19 blog (Queen Mary University of London – Criminal Justice Centre), 2 June 2020, <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/open-textured-legislation-in-the-times-of-covid-19-reasonable-excuse-and-legal-certainty.html>.
16 See, for example, the Laser Misuse (Vehicles) Act 2018; the Firearms Act 1968; Human Medicines Regulations 2012.
17 Consider the application of *Dolan and others*, [2020] EWCA Civ 1605, and *Leigh and others v Commissioner of the Police of the Metropolis,* [2021] EWHC 661 (Admin).
18 For example, the Health Protection (Coronavirus, Restrictions) (All Tiers) (England) Regulations 2020 (SI 2020 No. 1374, as amended by SI 2021 No.8).
19 Para. 2(2), Schd. 3A; Health Protection (Coronavirus, Restrictions) (All Tiers) (England) Regulations 2020 (SI 2020 No. 1374, as amended by SI 2021 No. 8).
20 See R. Fortson, 'Conflating "Guidance" and "Rules"– Restrictions on "Exercise" during the Jan 21 Covid Lockdown', Responding to Covid-19 blog (Queen Mary University of London – Criminal Justice Centre), 14 January 2021, <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/conflating-guidance-and-rules---restrictions-on-exercise-during-the-jan-21-covid-lockdown.html>.
21 BBC News online: 'Covid: Women fined for going for a walk receive police apology', <https://www.bbc.co.uk/news/uk-england-derbyshire-55625062>.
22 A deeply troubling consequence of the COVID-19 lockdown is the reported incidence of domestic violence and other abuses: see E. Lynch and E. Guild, 'The impact of increasing domestic violence as a result of COVID-19 on those with insecure immigration status', Responding to Covid-19 blog (Queen Mary University of London – Criminal Justice Centre), 22 July 2020, <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/the-impact-of-increasing-domestic-violence-as-a-result-of-covid-19-on-those-with-insecure-immigration-status.html>; see also the Office for National Statistics, 'Domestic abuse during the coronavirus (COVID-19) pandemic, England and Wales: November 2020'; and J. Kelly, 'Coronavirus: Domestic abuse an "epidemic beneath a pandemic"', BBC News, 23 March 21, <https://www.bbc.co.uk/news/uk-56491643>.
23 Specifically, regulation 6 of the Health Protection (Coronavirus, Restrictions) (England) Regulations (SI 2020/350).
24 [2020] EWHC 2962 (Admin).
25 <https://www.cps.gov.uk/cps/news/cps-review-findings-first-year-coronavirus-prosecutions>. The CPS point out that the figures are provisional.
26 <https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/1364/136408.htm#_idTextAnchor018>, para. 57.
27 Noting section 10 of the Human Rights Act 1998: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."
28 For example, consider s. 336 of the Companies Act 2006 that requires every public company (s. 336(1)) and every private "traded company" (s. 336(1A)) to hold an Annual General Meeting. A failure to comply with s. 336(1) or (1A) is an offence: s. 336(3): see section 37 and Schedule 14 of the Corporate Insolvency and Governance Act 2020 that, for a limited period, permitted Annual General Meetings to be held, and for any votes to be cast, "by electronic means or any other means" (schedule 14, para. 3).
29 With particular reference to Arts. 5, 6 and 7 of the ECHR and Human Rights Act 1998.
30 S. Carrera, V. Mitsilegas and M. Stefan, 'Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age', *Centre for European Policy Studies (CEPS),* Brussels May 2021, <https://www.ceps.eu/ceps-publications/criminal-justice-fundamental-rights-and-the-rule-of-law-in-the-digital-age/>.
31 The expression "achieving best evidence in criminal proceedings" has been something of a mantra that has been uttered by policy makers in England and Wales for several years: see, for example, 'Achieving Best Evidence in Criminal Proceedings: Guidance on interviewing victims and witnesses, and guidance on using special measures', Ministry of Justice, 2011: <https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/best_evidence_in_criminal_proceedings.pdf>
32 Defined by section 56(2) of the CJA 2002 as, "a live television link or other arrangement by which a witness, while at a place in the United Kingdom which is outside the building where the proceedings are being held, is able to see and hear a person at the place where the proceedings are being held and to be seen and heard by the following persons."
33 Section 51(1B), CJA 2003 as substituted by the CA 2020, schd. 23, para. 2.
34 Section 51(1), CJA 2003 as substituted by the CA 2020, schd. 23, para. 2.
35 Section 51(2), CJA 2003 as substituted by the CA 2020, schd. 23, para. 2.
36 Section 56(2B), CJA 2003 as substituted by the CA 2020, schd. 23.
37 Section 56(2D), CJA 2003.
38 Section 51(4), CJA 2003 as substituted by the CA 2020, schd. 23, para. 2.
39 Section 51(4), CJA 2003 as substituted by the CA 2020, schd. 23, para. 2.
40 Section 51(6), CJA 2003 as substituted by the CA 2020, schd. 23, para. 2.
41 "Those circumstances include in particular (a) in the case of a direction relating to a witness – (i) the importance of the witness's evidence to the proceedings; (ii) whether a direction might tend to inhibit any party to the proceedings from effectively testing the witness's evidence; (b) in the case of a direction relating to any participant in the proceedings – (i) the availability of the person; (ii) the need for the person to attend in person; (iii) the views of the person; (iv) the suitability of the facilities at the place where the person would take part in the proceedings in accordance with the direction; (v) whether the person will be able to take part in the

proceedings effectively if he or she takes part in accordance with the direction."
42 See s. 51(4B) and schedule 3A of the CJA 2003 (as modified by the CA 2020).
43 Section 54(2), CJA 2003 as substituted by the CA 2020.
44 By having inserted Part 3A into the Crime and Disorder Act 1998.
45 Section 57A(1) of the Crime and Disorder Act 1998 as modified by the CA 2020.
46 Sections 57B, s. 57E and s. 57F (respectively) of the Crime and Disorder Act 1998 as modified by the CA 2020.
47 Much has been written on this topic. Consider, for example, M. Stone, 'Instant lie detection? Demeanour and credibility in criminal trials', [1991] Crim. L.R., 821–830; J.R. Spencer, 'Orality and the evidence of absent witnesses', [1994] Crim.L.R., 628–644; S. Phillimore, 'Credibility versus demeanour – the impact of remote court hearings', (2020) 50 Fam. Law, 971–972; Q. Amna, 'Relying on Demeanour Evidence to Assess Credibility during Trial – A Critical Examination' (January 1, 2014), SSRN: <https://ssrn.com/abstract=2384966> or <http://dx.doi.org/10.2139/ssrn.2384966>.
48 Readers must not be confused by the expression "soft law" as used by *Sorabji* and *Vaughan*. The guidance did not constitute actual law but it carried considerable persuasive authority having been given by senior judges such as the Lord Chief Justice.
49 J. Sorabji and S Vaughan, '"This Is Not A Rule": COVID-19 in England & Wales and Criminal Justice Governance via Guidance', (2021) 12 *European Journal of Risk Regulation*, 143–158.
50 [2020] EWHC 2167 (QB).

The COVID-19 Pandemic as a Stress Test on the Right to Protection of Personal Data

The Case of Greece

Niovi Vavoula

This article aims to critically examine the limitations to the fundamental right of personal data protection in Greece by exploring three instances in which the rules and practices have put the protection of personal data under significant pressure: (1) the processing of information on individuals who obtain movement permits via SMS; (2) the tracking of COVID-19 patients; and (3) the guidelines on the management of the COVID-19 crisis by the Hellenic Data Protection Authority (DPA). The article argues that the Greek response to COVID-19 has been fraught with over-restrictive measures that go beyond what is necessary and proportionate in a democratic society. In particular, the requirement of obtaining movement permits via SMS, which has been inserted through soft law, thus without parliamentary scrutiny, has relativized data protection and has lowered individuals' resistance to future surveillance practices marking everyday movement as a matter of interest to the state. In relation to contact tracing the article demonstrates that an excessive retention period of patients' data is foreseen. As for the DPA's guidelines on the processing of personal data within the framework of COVID-19 it is concluded that they have provided an unclear and overly permissible interpretation of the GDPR rules in favour of the state.

I. Introduction

The current COVID-19 pandemic is affecting our lives in an unprecedented manner and constitutes an intense crash test of a series of fundamental rights.[1] During the first few months of the pandemic, Greece emerged as the EU's poster child in tackling the spread of COVID-19. The Greek response entailed significant limitations on the exercise of fundamental rights, aiming in particular at the freedom of movement and assembly, economic freedom, and the exercise of freedom of religion. Concerns were voiced, particularly when the freedom of assembly and religion were in question. Although trust in political institutions may have been shaken, legal scholars have conceded that, in the context of the temporariness of the limitations and the public health interest at stake, the extreme limitations to these rights did not affect Greek democracy and the rule of law.[2]

This article aims to critically examine in depth the limitations to the fundamental right of personal data protection, especially as enshrined in Art. 8 of the Charter and in Art. 9A of the Greek Constitution.[3] Personal data protection has received relatively modest attention in comparison to other fundamental rights.[4] To this end, the article explores three instances in which the Greek rules and practice put the protection of personal data under significant pressure:

- The processing of information on individuals who obtain movement permits via SMS;
- The tracking of COVID-19 patients;
- The guidelines on the management of the COVID-19 crisis by the Hellenic Data Protection Authority (DPA).

II. Movement Permits via SMS: The Relativisation of the Right to Personal Data Protection

Throughout the pandemic, Greece has reacted swiftly by imposing restrictions on freedom of movement and other measures of social distancing. In particular, the Greek government first issued a ban on all unnecessary traffic from 23 March 2020, which lasted until 4 May 2020. Similar restrictions on movement of varying degrees and intensity were further imposed during the second and third waves of the pandemic on 1 November 2020 and continue to apply with less intensity to date. Restrictions on freedom of movement have gone hand-in-hand with efforts to monitor those on the move, as well as their personal associations if they have become infected. In a unique approach to handling the pandemic, during periods of lockdown and until 15 May 2021, anyone on the move falling within one of the six expressly listed exceptions has been required to carry an identification document and a movement permit. They could be obtained by filling out an online form, or – certainly the most popular option – by sending a mobile message to a dedicated number operated by the General Secretariat of Civil Protection (Γενική Γραμματεία Πολιτικής Προστασίας), a public law body that belongs to the Ministry of Citizen Protection. To obtain permission via SMS, the individual was required to provide his/her name and surname, residence address, and a code number corresponding to the purpose of movement. In the event of a random check by the police, individuals were required to show their movement permit; otherwise a fine could be imposed. Possible exceptions were the following: visits to pharmacy or doctor following an appointment (code number 1); supermarket/minimarket (code number 2); bank (code number 3); to help someone at home (code number 4); attending a funeral (code number 5); and physical exercise outdoors (code number 6).[5]

After sending the initial SMS, individuals immediately received an SMS with their movement permit. This did not apply to employees or self-employed persons who had to carry specific paperwork with them. During periods when Greece imposed restrictions on movement after a specific hour in the evening, all code numbers, except 1 and 6 (only in relation to taking out a pet), did not permit movement. Otherwise, there were no other restrictions as to how many movement permits a person may request per day, as long as the general lockdown rules were followed. This is a novelty of Greece; no other EU Member State has used this anti-COVID strategy, with the exception of Cyprus, where the rules were similar.[6] In January 2021, a cautious easing of the second lockdown was attempted and retail stores reopened, whereby consumers could only shop for two hours per day by making an appointment via SMS and showing a written confirmation of the electronic purchase, if applicable. In April 2021, stores reopened once again following the same rules, but by 15 May 2021 all requirements regarding movement permits were lifted.

Notably, although an abundant amount of ministerial decisions has been adopted in the context of the pandemic, the rules on the processing of personal data in the context of movement permits have not been laid down in law. Instead, the General Secretariat for Civil Protection merely released a "data protection policy" online, in the form of "soft law,"[7] without prior scrutiny, consultation, or transparency. The government opted for this approach, despite the possible implications it posed for the legality of data processing and the impact for individuals whose information is processed. The policy is written in Greek only, which does not enable foreigners living in the country to obtain information as to how their personal data are processed. The policy explicitly proscribes centralised storage and thus data must be deleted immediately. However, data can be anonymised for statistical use. Therefore, after an individual would receive an SMS message with a movement permit, his/her data are either deleted or anonymised.

One could argue that, because of the limited timeframe during which the measure applied and the deletion of data after issuance of the movement permit, there was no need for further formalisation of the rules. Perhaps this explains why the data protection policy in relation to the movement permits was suspended between the end of the first lockdown and the beginning of the second one and was located online only throughout the duration of the measures. This policy has raised significant concerns, however, due to the use of legal language that may not understandable and accessible to the layperson, the lack of reference that sensitive data are collected (as one of the exceptions permitting movement is a doctor's appointment), the confusion as to whether the information submitted by individuals could be submitted to third parties and, in general, as to who the recipients of the information contained in an SMS are.[8] Furthermore, Art. 13 of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) requires that persons whose personal data are processed must be informed about the purposes of the data processing and the details of the data protection officer, which are missing from the Greek policy.[9]

More worryingly, in November 2020, it was made known that an automatic decision refusing a movement permit is possible

in cases of an increased number of messages coming from certain geographical areas. This automated individual decision-making significantly affects the legal position of individuals. According to Art. 22(2)(b) of the GDPR, such automated decision-making may take place *inter alia* if authorised by a Member State. However, safeguards must be laid down in such cases, at least "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." This has not been the case here.

Lastly, doubts as to whether SMS data are anonymised or remain personalised have also been voiced; whereas it may be useful for the administration to know how many people send an SMS invoking a particular exception as a reason for movement, it is worrying that, in the case of protest that took place in front of the American Embassy in November 2020, it became known to the authorities which reason of movement the demonstration participants had used to obtain their movement permit.[10] This is particularly worrying if one considers the fact that, even if data are anonymised for statistical purposes, it is still unclear how it was possible to isolate that data by proximity to a specific location.

Overall, this lack of transparency and clarity in the elaboration of the data protection policy raises significant issues of unlawfulness and circumvention of the legislative process, even though criticism against the content of the data protection policy was raised during the first wave of the pandemic. By elaborating the data protection policy through soft law, the importance of the rights to the protection of personal data has been significantly downgraded, the right has essentially been relativized, and a negative precedent for normalised, unlawful processing of personal data *en masse* was thus created. Looking at the bigger picture, the use of movement permits may signify a detrimental mind shift that citizens' legitimate, everyday activities are also of interest to the state, thus increasing the social acceptance of other, more intrusive surveillance practices in the future.

III. Proportionality Concerns through the Tracking of COVID-19 Patients

The analysis above showcases how technological means have been a crucial component in efforts to contain the spread of the virus and protect public health, raising significant privacy and data protection concerns. Nowhere has the evolution of technology been more relevant in responding to COVID-19 than in so-called "exit strategies," particularly apps and other tools to trace and track the contacts of persons suspected of or diagnosed with COVID-19.[11] At the time of writing, the Greek government was still in the process of evaluating the different application models that have been proposed over the past several months, and a contact tracing app is still in the development phase.[12]

In the meantime, contact tracing takes place through traditional means of collection of patient data. Such collection has been mandated by acts of legislative content. In particular, Art. 5 of the Act of Legislative Content (Πράξη Νομοθετικού Περιεχομένου) of 14 March 2020[13] mandated the collection of personal data of potentially or actually infected persons by the Hellenic National Public Health Organisation (Εθνικός Οργανισμός Δημόσιας Υγείας, Ε.Ο.Δ.Υ), a private law entity, with the aim of sharing it with the General Secretariat for Civil Protection.[14] According to Art. 5(1) of the Act, the data shared include the person's name, gender, age, contact number, full address, information on whether he/she has been hospitalised and, if so, in which hospital, and, where relevant, the place of self-isolation. The data are pseudo-anonymised and its transmission encrypted; processing of the data is limited to the purposes of coordination between the Hellenic National Public Health Organisation and the General Secretariat for Civil Protection for the effective fight of COVID-19. In terms of the data retention period, Art. 5(2) of the Act foresees the storage of collected data for the duration of the urgent measures.

In addition, Art. 29 of the Act of Legislative Content of 30 March 2020 established a National Registry of COVID-19 patients, which regulates the processing of personal data and individual rights.[15] The Ministry of Health issued a Ministerial Decision on 14 April 2020 for the implementation of said registry. According to Decision No. 2650 of 10 April 2020 of the Ministers of Health and Digital Governance that was issued later, the data are to be kept almost indefinitely, as they can be retained for 20 years after the individual's death.[16] The lack of proportionality of this provision, which is in line with the overall restrictive nature of measures adopted by the Greek government in handling the pandemic, is striking.[17] It may be recalled that, in a series of judgments, both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) clarified that the temporal character of data retention is an important element for the proportionality test. In *S and Marper v. the United Kingdom*, the ECtHR emphasised that the indefinite retention of sensitive personal data, irrespective of their further use, may have a direct impact on the applicants' private life interests, including their stigmatisation.[18] Furthermore, in *Digital Rights Ireland*, the CJEU opined that the retention period must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[19]

In the present case, the long retention period is equated with indefinite retention, which, in keeping with the relevant case

law, is disproportionate, particularly when the COVID-19 pandemic ends. Importantly, the retained data include information on the health of individuals, which qualifies as a special category of personal data according to Art. 9 of the GDPR. It is true that Art. 9 of the GDPR enables the processing of health data for various reasons, including reasons of public interest, but the end of the pandemic and thus the state of emergency will not justify the extensive retention period in any way. As for the contact tracing of individuals, this process is carried out by a designated centre situated in police headquarters. The process involves asking questions regarding the recent contacts of persons infected or suspected of being infected with the coronavirus. In order for public bodies (especially hospitals and clinics) to assess who constitutes a close contact and therefore must be subjected to a specific set of instructions due to the high risk of contracting COVID-19, the Hellenic National Public Health Organisation (EODY) circulated detailed guidelines specifying the relevant criteria about close familial and personal relations and associations.[20] These guidelines have also been made publicly available on the dedicated website of EODY, without elaboration in an administrative act.

IV. Hellenic Data Protection Authority to the Rescue?

A third example of how the right to the protection of personal data has taken a significant hit during the management of COVID-19 derives from the Hellenic Data Protection Authority (DPA). On 18 March 2020, the DPA issued guidelines on the processing of personal data within the framework of COVID-19, particularly as regards the applicability of the GDPR.[21] The DPA is an independent authority entrusted with various tasks in accordance with Arts. 51–59 of the GDPR, including the issuance of opinions on its own initiative or upon request on any issue related to the protection of personal data.[22] From time to time, the DPA issues soft law in the form of guidelines suggesting solutions to various problems arising from the advancement of new technologies. In this context, the DPA COVID-19 guidelines focus on the use of personal data including health data by both public and private bodies, especially in the employment field and in relation to media reporting and coverage. The DPA has provided a definition of health-related data, which includes naming or identifying a data subject as a patient, staying at home due to illness, and finding signs of illness based on clinical symptoms (cough, nasal discharge, body temperature higher than normal, etc.).[23] According to the DPA, such information falls within the realm of the GDPR only when processed wholly or partly by automated means and not when provided orally.[24] Therefore, the DPA guidelines are far from technical in nature and provide an interpretation of the GDPR in numerous respects.

In addition, the DPA states a series of applicable legal bases for the processing of personal data for COVID-19 related purposes,[25] provided that basic principles are met and that relevant substantive and procedural safeguards and conditions for lawful processing are ensured.[26] The DPA further emphasises the processing of personal data by the private sector within the framework of employment relationships. It opined that, insofar as the GDPR applies, employers are entitled to process personal data in order to protect the health of employees. As a result, the following practices are explicitly allowed: measuring the body temperature of incoming individuals; submitting questionnaires regarding the health status of employees or their relatives; requesting travel history; informing other employees of the fact that a fellow employee has been infected; exposing the employee's identity.

It is noteworthy that, in view of the "critical and unprecedented time," the DPA stressed that no policy choice could be excluded from scrutiny outright. However, the key data protection principles, as enshrined in Arts. 5 and 6 of the GDPR, are applicable. Thus, the DPA rightly noted that extensive collection of personal data resulting in profiling of employees does not comply with the principle of proportionality.[27] As has been pointed out, the guidelines are not particularly clear, and, in comparison to guidelines provided by national DPAs in other EU Member States, the Greek approach is somewhat overly permissive.[28] Another example of the ambivalent language used by the Greek DPA is a guideline according to which the transfer of information relating to the health status of individuals is prohibited "where it is creating a climate of prejudice and stigma, while it is also likely to have a preventative effect with regard to complying with the measures announced by the competent public authorities undermining eventually their effectiveness."[29] As a result, the DPA's view seems to have been influenced by the state of emergency and may have a considerable impact on the rights to respect for private life and the protection of personal data.

V. Concluding Remarks

The current COVID-19 pandemic is not only a health, economic, and social challenge but also a major challenge for national constitutions, international law, and the EU legal order. This article aimed to highlight how management of the pandemic has put the right to the protection of personal data to the test, even though Greece remains one of the few EU Member States in which a contact tracing app has not become operational yet. Although the debate about the constitutionality of harsh restrictions of rights due to the priority of public health interests and the exceptional character of the measures holds merit,[30] the present analysis has highlighted the sharp

contrast between the constitutional protection of the right to data protection and the elaboration of rules that affect individuals on a daily basis outside the legislative procedure. Furthermore, despite the exceptional character of the limitations, certain (disproportionate) rules or the restrictive interpretation of rules may have wider, long-lasting implications on the protection of personal data. It remains to be seen whether the right to data protection has taken an irreversible hit.

Dr. Niovi Vavoula
Lecturer in Migration and Security, School of Law, Queen Mary University of London

1 For example, see EU Agency for Fundamental Rights, "Coronavirus pandemic in the EU – Fundamental Rights Implications: Focus on social rights" (November 2020).
2 G. Karavokyris, "Constitutionalism and COVID-19 in Greece: The Normality of Emergency", *Verfassungsblog* <https://verfassungsblog.de/constitutionalism-and-covid-19-in-greece-the-normality-of-emergency/> accessed 9 May 2021.
3 Art. 9A stipulates: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law."
4 This contribution is an updated and expanded version of E. Tsourdi and N. Vavoula, "Killing me Softly? Scrutinising the Role of Soft Law in Greece's Response to COVID-19", (2021) 21 *European Journal of Risk Regulation*, 59.
5 "SMS authorization for movement during lockdown back", *e-Kathimerini*, 5 November 2020 <https://www.ekathimerini.com/news/258853/sms-authorization-for-movement-during-lockdown-back/> accessed 9 May 2021.
6 In Cyprus, the regulatory framework of permits was different, as every individual had the possibility to receive only two permits per day.
7 General Secretariat for Civil Protection, "Personal Data Policy" (Section 4) <https://forma.gov.gr/docs/data-protection-policy.pdf> (in Greek), accessed 9 May 2021.
8 For concerns, see "Open Letter", *Homo Digitalis* <https://www.homodigitalis.gr/wp-content/uploads/2020/04/%CE%95%CF%80%CE%B9%CF%83%CF%84%CE%BF%CE%BB%CE%AE_%CE%A0%CE%BF%CE%BB%CE%A0%CE%94_13033_HD_30.03.2020.pdf> (in Greek), accessed 9 May 2021.
9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L 119, 4.5.2016, 1.
10 "Τα προσωπικά μας δεδομένα απροστάτευτα στο 13033", *OSARENA* <https://osarena.net/ta-prosopika-mas-dedomena-aprostateyta-13033/> accessed 9 May 2021.
11 For an analysis on tracking apps in the EU, see H. van Kolfschooten and A. de Ruijter, "COVID-19 and Privacy in the European Union: A Legal Perspective on Contact Tracing" (2020) 41(3) *Contemporary Security Policy*, 478. For a comparative study, see EU Agency for Fundamental Rights, "Coronavirus Pandemic in the EU – Fundamental Rights Implications: With a Focus on Contact-Tracing Apps" (April 2020).
12 See European Commission, "Mobile contact tracing apps in EU Member States" <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en> accessed 9 May 2021.
13 The Greek Constitution does not provide for a state of emergency. Instead, it establishes the notion of an "act of legislative content" (Ράξη νομοθετικού περιεχομένου), on the basis of which the Greek government has adopted general measures in response to the COVID-19 pandemic. For concerns on this approach, see E Fasia, "Effective but Constitutionally Dubious: The Constitutionality of Greece's Response to the Pandemic", *Verfassungsblog* <verfassungsblog.de/effective-but-constitutionally-dubious/> accessed 9 May 2021.
14 Act of Legislative Content, "Emergency measures in response to the need to limit the dispersion of the coronavirus COVID-19" OG A' 64/14-3-2020 <www.dsanet.gr/Epikairothta/Nomothesia/PNP_14-3-2020.htm> accessed 9 May 2021.
15 Act of Legislative Content, "Measures to tackle coronavirus COVID-19 pandemic and other urgent provisions" OG A '75/30-3-2020 <www.dsanet.gr/Epikairothta/Nomothesia/pnp30032020.htm> accessed 9 May 2021.
16 Joint Ministerial Decision 2650/10.04.2020 "Settlement of more specific technical issues for the operation of the National Patient Register for COVID-19, in accordance with the provisions of article twenty-nine of the Act of 30.3.2020 of the Legislative Content Act (PNP) 'Measures to deal with the pandemic of the corona COVID-19 and other urgent provisions' (A΄ 75) and 83 of Law 4600/2019 (A΄ 43)" OG B 1298/10.4.2020 <https://www.e-nomothesia.gr/kat-ygeia/astheneies/koine-upourgike-apophase-2650-2020.html> (in Greek), accessed 9 May 2021.
17 For criticism, see "COVID-19 και Ψηφιακά Δικαιώματα στην Ελλάδα" (COVID-19 and Digital Rights in Greece), *Homo Digitalis* <https://www.homodigitalis.gr/wp-content/uploads/2020/04/HomoDigitalis_Report_COVID19_and_Digital_Rights_in_Greece_22.04.2020_Final.pdf> accessed 9 May 2021.
18 ECtHR, 4 December 2008, *S and Marper v UK*, Application nos. 30562/04 and 30566/04, paras 107–121.
19 ECJ, 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12) para. 64.
20 "Handling COVID-19 patients' contacts" *EODY* <https://eody.gov.gr/wp-content/uploads/2020/03/covid-19-diaxeirisi-epafon.pdf> (in Greek), accessed 9 May 2021.
21 Greek Data Protection Authority, "Guidelines on Processing of Personal Data in the Context of the Management of COVID-19" (18 March 2020) <https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/NEWS/FILES/HELLENIC%20DPA_GUIDELINES_PROCESSING%20OF%20PERSONAL%20DATA_COVID-19.PDF> (in English), accessed 9 May 2021.
22 Art 57(3)(b) of the GDPR.
23 DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para. 1.
24 DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para. 2.
25 Specifically, Arts. 6(1)(c), 6(1)(d), 6(1)(e) as well as 9(2)(b), 9(2)(e), 9(2)(h) and 9(2)(i) of the GDPR.
26 DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para. 4.
27 DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para. 6.
28 Only the Greek and Belgian DPAs have adopted such an approach. For a comparative overview, see E. Pappa, "Κορωνοϊός, Θερμομέτρηση και Προστασία Προσωπικών Δεδομένων" (Coronavirus, Temperature Checks and Protection of Personal Data), *Lawspot* <https://www.lawspot.gr/nomika-blogs/evelina_pappa/koronoios-thermometrisi-kai-prostasia-prosopikon-dedomenon> (in Greek) accessed 9 May 2021.
29 DPA, COVID-19 Guidelines, *op. cit.* (n. 21), para. 9.
30 E. Venizelos, "Pandemic, Fundamental Rights and Democracy – The Greek Example" <https://evenizelos.gr/other-languages/375-articles-eng/6235-ev-venizelos-pandemic-fundamental-rights-and-democracy-the-greek-example.html> accessed 9 May 2021.

Dealing with Uncertainties in the Pandemic

A German Perspective

Katrin Kappler

The uncertainties experienced throughout the COVID-19 pandemic have posed major challenges both to the law itself and to its application. Prognostic uncertainties and gaps in knowledge about the new virus, on the one hand, and the need to act quickly, on the other, confronted the legislator and administrative courts with a challenge that could not be fully met by applying the hitherto existing Infection Protection Act. This contribution examines the legal responses to dealing with such uncertainties and illustrates them with examples of how the pandemic was handled in Germany. The focus is on aspects of legislation, followed by an analysis of the possibilities for judicial review of legislative decisions taken under uncertainty.

I. Introductory Remarks

More than a year ago, the global pandemic caused by the infectious coronavirus disease (COVID-19) also made its way to Germany. Since the first case became known on 27 January 2020, we have been struggling with the permissible legal responses to the pandemic, even though we were well prepared from a legal point of view: Germany had a legal framework for infectious diseases even before the outbreak of the COVID-19 pandemic, with the Infection Protection Act (*Infektionsschutzgesetz*) at its heart. This law enables the health authorities to adopt measures to combat the spread of a disease. It formed the legal basis by which to authorise the measures taken during the pandemic. It turned out, however, that this initial legal basis was effective for a transitional period only. As the pandemic continued to last longer, changes were needed to put the measures, which deeply interfere with fundamental rights, on a sound, longer-term legal basis. In the process, prognostic decisions had to be made that were influenced by scientific uncertainties concerning this new type of virus. This article aims to examine the mechanisms that German law provides to deal with these uncertainties.

II. Knowledge Deficits as a Key Challenge – Legal Responses

In the state apparatus, knowledge[1] has the function of guiding state action.[2] Especially in many areas of administrative law, decisions must be made under uncertainty.[3] At least two different dimensions of uncertainty must be differentiated here: First, prognostic legal decisions are always subject to epistemological uncertainties.[4] This is true even for a police danger prognosis in a simple case, since a certain degree of uncertainty always remains. Second, legal decisions on legal facts may require the incorporation of expert knowledge.[5] This is evident, for example, in the case of new technologies.

1. Uncertainties in infectious disease law

Infectious disease law is another example of a legal area in which decisions have to be made under uncertainty.[6] During a pandemic, science, politics, the media, and the law are confronted with a high degree of non-knowledge.[7] Moreover, experiential knowledge from previous pandemics is only of limited use in addressing these knowledge gaps, because each virus can be unique and therefore raises a specific set of questions.[8] The COVID-19 pandemic has confirmed this once again because additional and new knowledge gaps emerged. Some of the questions could only be answered in the course of the pandemic; others are still open or at least controversial.[9] At the beginning of the pandemic, for example, it was not clear beyond reasonable doubt whether wearing masks mandatorily would help contain the pandemic. In the meantime, compulsory mask wearing has been recognised as a central means of combating the pandemic. Unanswered questions still remain, however, about transmission of the virus, protection against the virus, and duration of the disease, for which there is not yet sufficient scientifically validated data due to the novelty of the virus.[10] At the same time, there is enormous pressure to act, because important legal interests can be affected by a pandemic and the overload of the health system is a persistent concern.[11]

2. The role of the Robert Koch Institute as an authority for knowledge processing and knowledge bundling

Knowledge infrastructures have been created in response to knowledge gaps and the complexity of processing knowl-

edge.[12] One example is the Robert Koch Institute (RKI). The Institute acts as a federal authority of the German Federal Ministry of Health at the intersection of science and politics. Thus, the Institute has the task of developing and conducting epidemiological and laboratory-based analyses as well as research on the cause, diagnosis, and prevention of infectious diseases.[13] The Institute usually acts informatively and does not itself impose any rules. For example, the RKI issues reports on national infection statistics and the epidemiological situation on a daily basis. In addition, advice is published, e.g., treatment options or hygiene instructions.[14] However, it is possible that other decision-makers link legal consequences to the Institute's assessments, a classic example being the coronavirus risk areas. Classification as a risk area is made after joint analysis and decision by the Federal Ministry of Health, the Federal Foreign Office, and the Federal Ministry of the Interior. The classification of risk areas has an impact on persons entering Germany: if they have stayed in such a risk area at any time within the last 10 days prior to entry, they are obliged to isolate themselves in accordance with the respective quarantine regulations of the responsible *Länder*.

It turned out that the expertise of the RKI has been of crucial importance for the legislator as well as for the courts. It is regularly consulted as a source. The preparation of the state of knowledge and assessment of the risk situation facilitates the work in legislation and judicial proceedings. This is illustrated, for instance, by §§28a and 28b, which were inserted into the Infection Protection Act (further details below) and which link the adoption of protective measures against the spread of the coronavirus disease to the published infection figures of the RKI.

3. Suitability *(Geeignetheit)* and prerogative of assessment *(Einschätzungsprärogative)*

A central aspect of the constitutionality of a law is the question of proportionality,[15] namely whether the law pursues a legitimate purpose and whether it is suitable, necessary, and appropriate to achieve its purpose. During the pandemic, the suitability of measures has been an ongoing issue. An objective standard applies when assessing suitability.[16] It is therefore not a question of whether a public authority considers a measure to be suitable but rather whether a measure is actually suitable.[17] This is the case if it *promotes* the legitimate purpose at which the measure is aimed. It is not necessary that the goal is achieved.[18]

The suitability test is also the gateway for non-law expertise. Thus, the necessity requirement is always a gateway for interdisciplinary cooperation between lawyers and experts from other disciplines, e.g., from the fields of economics or science. This has also been clearly demonstrated throughout the pandemic. From the very beginning, the political and legal debate was supplemented with findings from the sciences, especially the knowledge and findings of epidemiologists.

Due to the novelty of the virus, however, the scientific community was also confronted with great uncertainties, as mentioned above. This is reflected in legislation. The law has an answer to such uncertainties: the legislature's prerogative of assessment.[19] German law generally confers on the legislator a broad prerogative of assessment but, at the same time, requires that this prerogative of assessment is supported by knowledge.[20] In other words, the extent of the prerogative depends on the existing state of knowledge. If there is little knowledge of an issue or if the findings are controversial, the prerogative of assessment is broad. This has also been emphasised by the courts during the pandemic. They regularly clarified that legislative decisions can only be reviewed to a limited extent.[21] According to the case law of the Federal Constitutional Court, the creative leeway is only exceeded if a consideration is so obviously flawed that it cannot reasonably form a basis for the measures taken.[22]

III. Uncertainties in Pandemic Legislation

Against this background, the following section analyses to what extent these principles have been adhered to in the current situation and whether they have served their purpose. After a brief introduction to the relevant provisions of the Infection Protection Act, two examples will illustrate how difficult it is to deal with knowledge in the legislative process and how far the legislature's prerogative of assessment extends. As a result, I will show that the prerogative of assessment is the central instrument for responding to the issue of uncertainty.

1. Legal bases of infectious disease law

The infectious disease law includes all regulations that govern the state's handling of infectious diseases. As mentioned in the introduction, the core of this legal area in Germany is the Infection Protection Act (*Infektionsschutzgesetz*). The Infection Protection Act regulates measures to prevent and control infectious diseases, including COVID-19. It is applicable irrespective of whether an epidemic or pandemic is involved. Throughout the COVID-19 pandemic, the provisions in the section on the control of an infectious disease have been key. This section operates with a general clause (*Generalklausel*) and standard powers (*Standardermächtigungen*). General clauses determine general requirements for a large number of measures that have not yet been specified in detail.[23] Standard

powers set conditions for a specific measure, such as the isolation (*Absonderung*) of sick persons in §30 of the Infection Protection Act. The general clause of §28 was particularly relevant. It stipulates that, if an infectious disease is detected, the competent authority "may take all necessary protective measures," i.e., it is granted discretionary powers. On the basis of this provision, various measures were taken in practice, e.g., bans on leaving or contact restrictions.

2. Amendments to the Infection Protection Act

The general clause can be used by the authorities if no further specific regulations are available to the legislature.[24] Due to the gaps in knowledge already described, it was necessary to base many – even far-reaching – measures on the general clause at the beginning of the pandemic. As the pandemic progressed, legal scholars increasingly criticised that the fact that the general clause was no longer sufficient for the profound interference with fundamental rights.[25] Courts have also shared these arguments.[26]

Therefore, the general clause in §28 of the Infection Protection Act has already been amended twice during the COVID-19 pandemic: In March 2020, it was supplemented by very extensive fundamental rights interventions, such as the curfew.[27] With the amendment in November 2020, the legislator has largely included the measures previously taken in the context of the COVID-19 pandemic in §28a of the Infection Protection Act. In so doing, it identified them as mere examples of measures that could be enacted under the general clause of §28(1) of the Infection Protection Act. As a result, the Infection Protection Act continues to deviate from the regulatory technique that is customary in security law, i.e., defining standard measures as independent authorising elements.[28] Some legal scholars argue that this exemplary enumeration is insufficient because the measures are still not linked to further-reaching elements.[29] These considerations probably stem from security law doctrine, which establishes that more restrictive prerequisites are needed for intervention-intensive measures; one example is that, instead of a danger, an *immediate* danger is required in general police law for flat searches.[30] In this context, however, it should be called to mind that even the standard powers in the Infection Protection Act are not always subject to stricter criteria. Furthermore, the legislature has a prerogative to assess the regulatory system, which has not been exceeded here.[31] The new provision in §28a of the Infection Protection Act only creates examples and not separate standards powers; the legislature clarified which measures it considers permissible and under which conditions they are permissible.[32] Thus, as with standards powers, recourse to the general clause is no longer possible without further ado.

3. First example: link to incidence rates in the Infection Protection Act

With the incorporation of §28a and §28b into the Infection Protection Act, incidence thresholds have also been added to the law. They are linked to the R-values published by the RKI. This once again demonstrates the importance of a specialised scientific institute when drafting legislation. The link to incidence rates (*Inzidenzwerte*) has been criticised in many respects.[33] I argue that the link to incidence rates is not generally impermissible, but the current regulations are poorly designed and unclear and therefore unconstitutional.

a) Content of the regulations and link to different incidence rates

§28a (3) of the Infection Protection Act states that if a threshold of more than 35 new infections per 100,000 inhabitants within seven days is exceeded, "broadly based protective measures" (*breit angelegte Schutzmaßnahmen*) are to be taken in order to rapidly reduce the incidence of infection. If a threshold rate of more than 50 new infections per 100,000 inhabitants within seven days is exceeded throughout the country, nationally coordinated "comprehensive protective measures" (*umfassende Schutzmaßnahmen*) must be taken that can be expected to effectively contain the incidence of infection. With the reform in mid-April 2021, §28b was inserted into the Infection Protection Act, which also refers to the incidence rate as a measure of frequency. However, two things are noteworthy here: First, the standard in §28b is exclusively linked to incidence rate, unlike §28a, which also includes the functionality of the health care system and the protection of life and health as substantial requirements. Secondly, the norm is self-executing. This means that the measure comes into force without any intervening state act, e.g., without the enactment of a law or a legal ordinance.

b) Suitability of the link to incidence rates

Legal scholars are in debate over whether it makes sense to use incidence rate in law at all. With regard to the legitimate purpose of including them, it was pointed out that relieving the burden on hospitals and intensive care units must be considered. Scientific findings indicate that COVID patients are getting younger and need to be treated there longer.[34] Even if the inclusion of incidence rates in the law is considered reasonable, this raises the question of which incidence thresholds should be meaningfully inserted into the law. In this context, *Kießling* points out that the link to an incidence rate of 100 is insufficient to effectively reduce the incidence of infection.[35] This may be scientifically correct, but it does not answer the question of whether the legislature's prerogative of assessment

has been exceeded. In my view, it is constitutionally unobjectionable to create a legal link to incidence rate. It is undisputed that the purpose of the regulations is to protect hospitals from overload, so the incidence rate alone cannot be decisive for this issue because, for example, the capacity of the intensive care beds is also a decisive factor. Nevertheless, the incidence rates reflect a trend in the pandemic's development, meaning that they provide at least an indication of which measures are necessary. Here, we should again recall the legislature's prerogative of assessment: it is necessary, but also sufficient, to promote the purpose of the legislation. This is the case here.

c) Link to published incidence rates of the RKI – influence on clarity and certainty of the law

Notwithstanding, friction regarding the clarity and certainty of a norm can arise when findings from other scientific fields are incorporated into well thought-out legislation . One example is §28b of the Infection Protection Act, which raises considerable concerns over specificity and clarity. In general, it is necessary that norm addressees can find out what the law requires from them without excessive effort.[36] The requirements for certainty and clarity are particularly high if the norm extensively interferes with fundamental rights. The link to incidence rate itself is unobjectionable from a constitutional point of view. This applies at the minimum if the state is authorised to adopt concrete measures on the basis of incidences. However, the limit of definiteness and clarity has been reached with §28b: No official announcement is made on the individual measures that ensue once certain thresholds are exceeded. Instead §28b of the Infection Protection Act is directly linked to the incidence thresholds published by the RKI. The legislator thus assumes that all citizens will visit the Institute's website every day to look at the figures relevant to them and to check whether the measures listed there apply to them. The measures only apply on the day after the next – citizens also need to keep that in mind to find out whether the measures came into force. This inevitably leads to great uncertainty as to which measures apply where and when – an untenable legal situation.

4. Second example: night-time curfews

The biggest dispute in Germany with regard to the proportionality of measures against the coronavirus disease occurred over night-time curfews. In the explanatory memorandum to the law, the German legislator pointed out that the curfew restrictions were necessary to prevent private gatherings with too many people and the resulting emergence of new infection hotspots. The legislator made reference to studies that underpin this assessment.[37] Legal scholars differ as to the question of whether the suitability test has been met. *Möllers*, for instance, points out that the legislator does not have to prove the necessity of measures in detail. He argues, however, that the burden of proof increases when an obviously less severe measure comes into question, namely contact bans.[38] *Kingreen* contends that the studies, by means of which the legislator intends to prove suitability, have been chosen selectively and that they are controversial.[39] He additionally asserts that even the selected studies indicate that curfews have a moderate effect at best, possibly even no effect at all, on the incidence of infection.[40]

It is indeed doubtful whether a night-time curfew is actually suitable for combating the pandemic and relieving the burden on the health system. However, it is precisely this uncertainty that justifies the broad prerogative of assessment on the part of the legislature. The only decisive factor is whether it is at all plausible that a night-time curfew leads to lower infection rates. In my view, this is not the case because the night-time curfew at least has an additional effect on private meetings and thus also on the infection rates.

This conclusion does not imply that the curfew is constitutional because examination of the proportionality requirement for suitability is followed by examination of the requirements for necessity and appropriateness (see above). A measure is considered necessary if no means is available which is milder but equally suitable. Legal scholars often refer to contact bans as a less intensive measure. Although contact bans are probably a milder necessary measure, effective enforcement mechanisms are also needed to make them an equally appropriate measure. It should be taken into account that, in the case of contact bans, the authorities can no longer check people in public and question them about their reasons to be outside. Instead, enforcement shifts into the private sphere, since the authorities have to carry out the checks in private rooms – a considerable invasion of privacy. This line of argument was also emphasised in a recent decision of the Federal Constitutional Court.[41] Another argument in favour of necessity is that the legislature has the prerogative to make an assessment in the context of necessity. As regards the requirement of appropriateness, there are many indications that a night-time curfew is unconstitutional.[42] The answer to this question would necessitate a longer analysis which is not possible within the scope of this article. It should be pointed out here, however, that "knowledge" is not the decisive factor but rather the weighing up of individual fundamental rights with public interests.

IV. Judicial Review in the Pandemic

Knowledge and knowledge deficits are not only relevant for legislation, but also for jurisprudence. According to German

legal doctrine, it is not necessary for judges to have the same level of knowledge as the legislator does when making a decision requiring a review of proportionality.[43] The courts are not supposed to put themselves in the place of the legislature but rather to check whether it has respected the limits of the law, in particular whether it is proportionate.[44] The courts must decide, however, whether a measure is suitable. This means that the courts are faced with the same knowledge deficits that the legislator had to cope with. In the COVID-19 pandemic, this became a crucial issue before German courts. Case law shows that, in particular, the necessity of the protective measures has been subject to critical judicial examination.[45] This is not surprising, as the authorities were extremely challenged during the first few months of the pandemic and, when in doubt, opted for more far-reaching and blanket measures rather than finely tuned and differentiated measures.[46] With increasing experience and a growing knowledge of the mechanisms of the spread of the virus, some measures have proven to be too excessive and have been corrected by the courts.[47] Notwithstanding, the courts very often referred to the legislature's prerogative of assessment and upheld measures even when their effectiveness was disputed. Conversely, case law has shown that judicial review can also be effective in the case of uncertainties and prerogatives of assessment, because the judicial control of reasonableness remains even in the case of knowledge deficits. Here, the judicial examination is not only a matter of factual knowledge but also of weighing up fundamental rights. Although uncertainties can be considered here, the core aim is to strike a careful balance between conflicting fundamental rights. Case law has made extensive use of this approach. It has been pointed out, for instance, that the freedom of assembly is one of the highest goods within the German constitution and therefore bans without exception are unconstitutional.[48] The authorities picked up on this and took other measures, which then proved to be – at least partially – lawful.[49]

V. Conclusion

The COVID-19 pandemic has posed major challenges to the law itself and to the application of the law in Germany. The Infection Protection Act is the central piece of legislation upon which measures against the spread of the pandemic could be based. Since this Act had been legally and practically irrelevant for many years, it had to be (rapidly) adapted to the emerging new health challenges. From a legal point of view, both decision-making pressure and uncertainties have been the major aspects in the legislative process. German law provides mechanisms to ensure that the legislature remains capable of acting, on the one hand, but, on the other, that judicial control nevertheless remains possible. This has proven its value in our recent challenging times.

Dr. Katrin Kappler
Post-doctoral researcher at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

1 On the concept of knowledge, see L. Münkler, "Wissen – ein blinder Fleck des Rechts? Aspekte eines Spannungsverhältnisses", in: L. Münkler (ed.), *Dimensionen des Wissens im Recht*, 2019, p. 3, 5–10; B. J. Shapiro, *A culture of fact*, 2000, p. 12; P.-T. Stoll, "Wissensarbeit als staatliche Aufgabe – Wissen als Leitbegriff für Reformüberlegungen", in: I. Spiecker gen. Döhmann and P. Collin (eds.), *Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts*, 2008, p. 34, 35–38.
2 B. Fassbender, "Wissen als Grundlage staatlichen Handelns", in: J. Isensee and P. Kirchhof (eds.), *Handbuch des Staatsrechts*, Band IV, 3rd ed. 2006, pp. 244–259.
3 C. Kremer, "Ungewissheit im Sicherheitsverwaltungsrecht", in: I. Augsberg (ed.), *Extrajuridisches Wissen im Verwaltungsrecht*, 2013, p. 195, 198.
4 See M. Goldhammer, "Zwischen Prophetie und Prognose – zur Eigenlogik der hoheitlichen Vorhersage", in. L. Münkler (eds.), *Dimensionen des Wissens im Recht*, 2019, p. 217, 228–231.
5 L. Münkler, *op. cit.* (n. 1), p. 14.
6 A. Klafki, *Risiko und Recht*, 2017, pp. 13–15.
7 H-H. Trute, "Ungewissheit in der Pandemie als Herausforderung", (2020) *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)*, 93.
8 H-H. Trute, *op. cit.* (n. 7), 93–95; A. Klafki, *op. cit.* (n. 6), p. 13.
9 H-H. Trute, *op. cit.* (n. 7), 95.
10 See <https://www.infektionsschutz.de/coronavirus/fragen-und-antworten.html>, accessed 12 May 2021.
11 O. Lepsius, "Vom Niedergang grundrechtlicher Denkkategorien in der Corona-Pandemie", *Verfassungsblog* <https://verfassungsblog.de/vom-niedergang-grundrechtlicher-denkkategorien-in-der-corona-pandemie/> accessed 12 May 2021.
12 See, generally, L. Münkler, *op. cit.* (n. 1), pp. 22–23.
13 Hollo, in: Kießling (ed.), *IfSG Commentary*, 2020, § 4, mn. 6–7.
14 An overview is available here: <https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/nCoV.html> accessed 12 May 2021.
15 G. Lübbe-Wolff, "The Principle of Proportionality in the Case-Law of the German Federal Constitutional Court", (2014) 34 *Human Rights Law Journal*, 12–17.
16 See, generally, G. Warg, "Prognosegrundlage bei der Gefahrenabwehr nach dem IfSG", (2021) *Neue Juristische Online-Zeitschrift (NJOZ)*, 257–260.
17 BVerfG, Official Case Reports, E 115, 276, 308; E 117, 163, 188.
18 H. Jarass, in: H. Jarass/B. Pieroth, *Grundgesetz für die Bundesrepublik Deutschland - Kommentar*, 16th ed., 2020, Art. 12, mn. 42.
19 See, generally, J. Bethge, "Wessen (Un-)Wissen? Zur Tatsachengrundlage der Einschätzungsprärogativ", in: L. Münkler (ed.), *Dimensionen des Wissens im Recht*, pp. 201–215.
20 B. Fassbender, *op. cit.* (n. 2), p. 254.
21 J. Bethge, *op. cit.* (n. 19), pp. 201–215; L. Münkler, *op. cit.* (n. 1), p. 21.
22 BVerfGE 30, 292, 317.
23 BVerfGE 105, 279 (305); A. Kießling, in: A. Kießling (ed.), *IfSG Commentary*, 2020, § 28, mn. 55–61.

24 R. Poscher, "Das Infektionsschutzgesetz als Gefahrenabwehrrecht", in: S. Huster and T. Kingreen (eds.), Handbuch Infektionsschutzrecht, 2021, pp. 117, 133.
25 See, for example, K.F. Gärditz and M.K. Abdulsalam, "Rechtsverordnungen als Instrument der Epidemie-Bekämpfung", (2020) Zeitschrift für das Gesamte Sicherheitsrecht (GSZ), 108, 109–110.
26 See, e.g., VGH München, Beschluss vom 29.10.2020, Az. 20 NE 20.2360, mn. 20.
27 A. Sangs, "Das Dritte Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite und Gesetzgebung während der Pandemie", (2020) Neue Zeitschrift für Verwaltungsrecht (NVwZ), 1780-1785.
28 R. Poscher, *op. cit.* (n. 24), p. 144.
29 H. Eibenstein, "Die (vertane) Chance des § 28a IfSG", (2020) COVuR, 856, 858–859.
30 See, e.g., § 36 of the Police Code Baden-Württemberg and § 45 of the Federal Police Act.
31 See H. Greve, "Infektionsschutzrecht in der Pandemielage – Der neue § 28a IfSG", (2020) *NVwZ*, 1786, 1788.
32 R. Poscher, *op. cit.* (n. 24), p. 144.
33 See, e.g., A. Kießling, "Stellungnahme zum Entwurf eines Vierten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite", BT-Drs. 19(14)323(6), pp. 3–5; H. Eibenstein, (2020) COVuR, *op. cit.* (n. 30), 858.
34 T. Kingreen, "Stellungnahme zum Entwurf eines Vierten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite", Ausschuss-Drs. 19(14)323(19), p. 9.
35 A. Kießling, *op. cit.* (n. 33), p. 4.
36 E. Denninger, "Die Polizei im Verfassungsgefüge", in: H. Lisken/E. Denninger, Handbuch des Polizeirechts, 6th ed., 2018, Chapter B, paras. 61–64.
37 BT-Drs. 19/28444, p. 12.
38 C. Möllers, "Stellungnahme zum Entwurf eines Vierten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite", Ausschuss-Drs. 19(14)323(2), p. 6.
39 T. Kingreen, *op. cit.* (n. 34), pp. 7–8.
40 T. Kingreen, *op. cit.* (n. 34), p. 8.
41 BVerfG, Decision of the First Senate of 5 May 2021, 1 BvR 781/21, para. 38.
42 See, e.g., F. Schmitt, "Die Verfassungswidrigkeit der landesweiten Ausgangsverbote", (2020) Neue Juristische Wochenschrift (NJW), 1626, 1627–1631.
43 B. Fassbender, *op. cit.* (n. 2), p. 254.
44 Ibid.
45 See, e.g., BVerfG, NVwZ 2020, 783.
46 R. Poscher, *op. cit.* (n. 24), p. 160.
47 Ibid.
48 BVerfG, NVwZ 2020, 711, 712.
49 R. Poscher, *op. cit.* (n. 24), p. 161.

Imprint

Impressum

Published by:
Max Planck Society for the Advancement of Science
c/o Max Planck Institute for the Study of Crime, Security and Law
(formerly Max Planck Institute for Foreign and International Criminal Law) represented by Director Prof. Dr. Ralf Poscher
Guenterstalstrasse 73,
79100 Freiburg i.Br./Germany

Tel: +49 (0)761 7081-0
Fax: +49 (0)761 7081-294
E-mail: public-law@csl.mpg.de
Internet: https://csl.mpg.de

Official Registration Number:
VR 13378 Nz (Amtsgericht Berlin Charlottenburg)
VAT Number: DE 129517720
ISSN: 1862-6947

Editor in Chief: Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Managing Editor: Thomas Wahl, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Editors: Dr. András Csúri, University of Vienna; Anna Pingen, Max Planck Institute for the Study of Crime, Security and Law, Freiburg; Cornelia Riehle, ERA, Trier
Editorial Board: Peter Csonka, Head of Unit, DG Justice and Consumers, European Commission Belgium; Francesco De Angelis, Lawyer, Brussels Belgium; Prof. Dr. Katalin Ligeti, Université du Luxembourg; Prof. Dr. Ralf Poscher, Max Planck Institute for the Study of Crime, Security and Law, Freiburg; Lorenzo Salazar, Sostituto Procuratore Generale, Napoli, Italia; Prof. Rosaria Sicurella, Università degli Studi di Catania, Italia
Language Consultant: Indira Tie, Certified Translator, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Typeset: Ines Hofmann, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Produced in Cooperation with: Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)
Layout: JUSTMEDIA DESIGN, Cologne
Printed by: Stückle Druck und Verlag, Ettenheim/Germany

The publication is co-financed by the European Commission, European Anti-Fraud Office (OLAF), Brussels

Subscription:
eucrim is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@csl.mpg.de.
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@csl.mpg.de.

For further information visit our website: https://eucrim.eu
or contact:
Thomas Wahl
Max Planck Institute for the Study of Crime, Security and Law
Guenterstalstrasse 73,
79100 Freiburg i.Br./Germany
Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)
Fax: +49(0)761-7081-294
E-mail: info@eucrim.eu

MAX PLANCK INSTITUTE
FOR THE STUDY OF
CRIME, SECURITY AND LAW