eucrim
2021 / 4
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Fresh Perspectives on Unresolved Problems in European Criminal/Administrative Law
Nouvelles perspectives sur les problèmes non résolus du droit pénal/administratif européen
Neue Sichtweisen auf ungelöste Probleme im europäischen Straf-/Verwaltungsrecht

2021/4 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

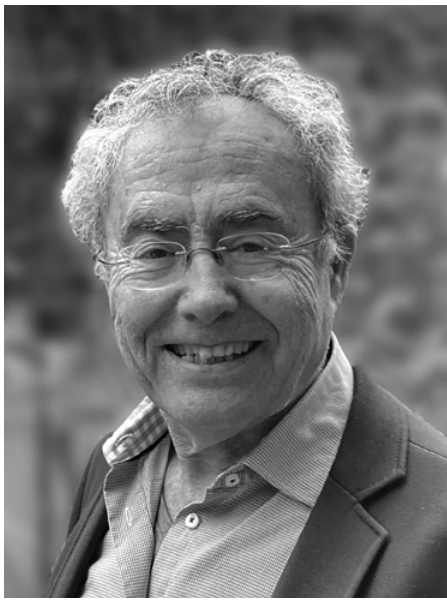
News*

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,



Francesco De Angelis

The front page of the eucrim issues published from 2006 to 2009 included the byline: "Successor to Agon". Indeed, to express the fight against fraud, the term "agon" (an ancient Greek term for "fight") had been chosen as the title of the original bulletin launched in April 1993 for the Associations of lawyers for the protection of the financial interests of – at that time – the European Community. The Associations were created following a landmark seminar in Brussels in 1989 that demonstrated the need for structures at the national level to bring together practitioners and academics and to provide a forum for their sensitization on the impact of European law on national criminal law. It is generally recognised that the Associations have been a catalyst for the development of European criminal law. In 1997, they released the Corpus Juris study containing the proposal to create a European Public Prosecutor and a European judicial area.

After productive reflection by and brilliant input from Professor *Ulrich Sieber* (Director of the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany) and Dr. *Lothar Kuhl* (Head of Unit at OLAF) a new forum, called eucrim, was launched in 2006. Today, eucrim is a remarkable publication, one that is well established in Europe, thanks in particular to the extraordinary work of Professor *Sieber* as Editor in Chief and *Thomas Wahl* as Managing Editor.

After having been responsible for the management of the bulletin Agon during my time at the European Commission and having been a member of the eucrim editorial board from its very beginnings, I recently resigned for reasons of "planned obsolescence". Since I now feel free as a bird, I would like to take the liberty to share some of my ideas on the future development and design of the eucrim project. First, I would like to call to mind the concept of eucrim, which is – and should remain – an indispensable instrument for all those operating in the area of European criminal law, particularly in the field of the "protection des interêts financiers" (PIF) of the European Union.

Eucrim serves as a forum for the Associations for the protection of the EU's financial interests and – as appears in the names of many Associations today – European criminal law. Their activities are financed as part of the EU's anti-fraud programme (best known under the name "Hercule") on the basis of annual calls for proposals managed by OLAF. Although OLAF manages the grants, however, it is indispensable that there be a driving force behind the Associations to broadcast and stimulate activities and to spark an innovative spirit. It is of paramount importance that the Associations feel a sense of belonging to a unique network integrated into the working strategy of the European Commission to address the protection of the Union's finances. At the same time, the network of the Associations can provide the Commission's services with valuable expertise and a wealth of practical experience from the Member States. Moreover, as representatives of civil society, the Associations are able to play a watchdog role in protecting democracy, especially in those countries in which the EU Charter of Fundamental Rights is under pressure. The fulfilment of the described configuration should tremendously motivate the network of eucrim correspondents to deliver regular contributions within the framework of eucrim's annual programme. The eucrim editorial team's challenging task of scouting for contributions would thus be enormously alleviated!

The reading audience genuinely appreciates eucrim's "News" section. It gives complete and in-depth information on the leading current developments in the European Union and the Council of Europe – a truly exclusive service for legal professionals and the general public thanks to the indefatigable work of *Thomas Wahl* and the eucrim editorial team!

According to its mission statement, eucrim was intended to "develop new visions and models for the European cooperation" (see also *Professor Sieber's* editorial in eucrim, 1–2/2006, 1). The guest editorials and the articles should both strive towards achieving these objectives. Guest editori-

als need not necessarily be linked to the "focus" of each issue (the recently introduced "fil rouge" serves this purpose). Editorials should express opinions that take strong, courageous positions and provoke interesting discussions.

The decision has been taken to expand eucrim beyond criminal law fields. This could be achieved, for instance, by exchanging ideas on the role of justice in the protection of EU-specific objectives. One of my proposals would be to depart from the (always excellent) ordinary path and step into more forward-looking debates, e.g. on the exciting field of climate change. I suggest including a section on "climate justice" to impart a vision of how to resolve and alleviate the unequal burdens created by climate change. In particular, the analysis of innovative national jurisprudence in this area could have a stimulating effect. At a time when EU money is being contributed to the Green Deal, which is at the top of EU policy, this section could address relevant questions of climate justice from human rights and environmental justice perspectives, while at same remaining closely linked with the protection of financial interests. eucrim could participate in the global debate and contribute actively to shaping minds! In its recent annual reports, OLAF has emphasised its role in protecting EU funds destined for the fight against climate change – further legitimation for eucrim to deal with this topic!

The articles in eucrim should be imbued with originality, which is always appreciated by the readers. It is worth investigating how to venture off the beaten track and confront topics that take a forward-looking approach like, for instance, granting the status of "electronic personality" to robots, who take autonomous decisions, learn from their own variable experience, and interact with third parties. In general, contributions should be dedicated to emerging topics that anticipate future problems. For example, it could become eucrim's core business to provide an in-depth analysis of possible future areas of competence for the European Public Prosecutor's Office, e.g. environmental law. I am firmly convinced that, after the initial triumphant announcements of success, our new European criminal law body will quite soon need further areas to investigate.

Ultimately, the editorial board is of paramount importance for eucrim's future, particularly to prevent eucrim from running the risk of becoming a routine-minded creature. The editorial board should be the "fulcrum" of eucrim and elaborate on future focal topics by way of "corporate democracy". There should be a constant exchange throughout the year among the members, with the obligation to take a position on any suggestion made by one of them in order to keep up an ongoing dialogue. I also suggest that the editorial board reflect on eucrim's role, objectives, design, layout (with more brilliant and intensive colours), tone, and targets in the light of a new security architecture at the European level and the challenges of a dramatically and constantly changing world.

May eucrim serve the European community for many years to come!

Francesco De Angelis, Lawyer,
eucrim Editorial Board Member (2006–2021)

News

Actualités / Kurzmeldungen*

European Union

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

Foundations

Fundamental Rights

2021 Report on Application of the Charter of Fundamental Rights in the EU

On 10 December 2021, the European Commission released its 2021 report on application of the Charter of Fundamental Rights in the EU. A special focus was on the challenges of protecting fundamental rights in the digital age. The 2021 report follows last year's strategy to strengthen application of the Charter of Fundamental Rights in the EU, including annual reports with thematic focuses (→eucrim news from 19 January 2021). The main issues raised in the report are as follows:

- Tackling the challenges of online content moderation: While online intermediaries, e.g. social media platforms, facilitate the exchange of information and play a major role in the democratic debate, the use of online platforms also amplifyies societal problems like polarization or the dissemination of illegal content, often with significantly negative effects on fundamental rights. The report noted that the revised Audiovisual Media Services Directive (AVMSD) – adopted in 2018 – includes measures to protect minors from audio-visual content and commercial communications that could cause them physical, mental, or moral harm. In 2016, the Commission signed a voluntary code of conduct with major online platforms to ensure that notifications of illegal racist and xenophobic hate speech are rapidly assessed (→eucrim 2/2016, p. 76). In addition, the Regulation addressing the dissemination of terrorist content online, which was adopted in 2021 by the European Parliament and the Council (→eucrim 2/2021, 95–97), ensures that terrorist content online is removed.
- Safeguarding fundamental rights when Artificial Intelligence (AI) is used: The report stressed that AI is frequently used without adequate safeguards and quality controls to automate or support decision-making processes or for surveillance activities that violate the rights of individuals. Bias in algorithms can lead to unjust and discriminatory outcomes. If AI is used in the context of law enforcement or the judiciary, it can also affect the presumption of innocence and the right to a fair trial and defence. The report pointed to the Commission proposal for a Regulation on AI presented in April 2021, which aims to ensure that high-risk AI systems are designed and used in compliance with fundamental rights;
- Addressing the digital divide: Not being online can affect people in the exercise of their rights. This is the case, for example, when political campaigns are increasingly run online. This can affect people's rights in a democratic society, including their right to freedom of expression and information. The digital divide has increased with the COVID-19 pandemic, as it has exacerbated these difficulties in accessing public services for those without the necessary technical equipment or digital knowledge. The report noted that various Member States are pursuing different approaches towards ensuring digital access to public services. It also stressed that efforts have been made at the EU level so that nobody is left behind (e.g. the Digital Education Action Plan launched in September 2020 or the European Electronic Communications Code).
- Protecting people working with platforms: While platform work has generated new economic opportunities for people, it also poses challenges to fundamental rights, including the protection of personal data, privacy, and fair and just working conditions. The report drew attention to the Commission's proposal for a directive to improve working

* Unless stated otherwise, the news items in the following sections (both EU and CoE) cover the period 9 October – 31 December 2021. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

eucrim – Common abbreviations

AFSJ	Area of Freedom, Security and Justice
AG	Advocate General
AML	Anti-Money Laundering
CBRN	Chemical, Biological, Radiological, and Nuclear
CCBE	Council of Bars and Law Societies of Europe
CCJE	Consultative Council of European Judges
CDPC	European Committee on Crime Problems
CEPEJ	European Commission on the Efficiency of Justice
CEPOL	European Police College
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
COSI	Standing Committee on Operational Cooperation on Internal Security
COREPER	Committee of Permanent Representatives
CTF	Counter-Terrorism Financing
DG	Directorate General
EAW	European Arrest Warrant
ECA	European Court of Auditors
ECB	European Central Bank
ECBA	European Criminal Bar Association
ECHR	European Convention on Human Rights
ECRIS	European Criminal Records Information System
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
EIO	European Investigation Order
EJN	European Judicial Network
ENISA	European Network and Information Security Agency
(M)EP	(Members of the) European Parliament
EPO	European Protection Order
EPPO	European Public Prosecutor's Office
EU	European Union
FCC	(German) Federal Constitutional Court
FD	Framework Decision
FT	Financing of Terrorism
GRECO	Group of States against Corruption
GRETA	Group of Experts on Action against Trafficking in Human Beings
ICTY	International Criminal Tribunal for the former Yugoslavia
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs
MoU	Memorandum of Understanding
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
ML	Money Laundering
OJ	Official Journal
OLAF	Office Européen de Lutte Anti-Fraude (European Anti-Fraud Office)
PNR	Passenger Name Record
SIS	Schengen Information System
SitCen	Joint Situation Centre
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

conditions for platform workers at the EU level by ensuring correct determination of their employment status.

The Commission calls on the European Parliament, the Council, and Member States to use this Annual Report on the Application of the EU Charter of Fundamental Rights to engage in exchanges about the challenges of and opportunities for protecting fundamental rights in the digital age. (AP)

Poland: Rule-of-Law Developments End of October to December 2021

This news item continues the overview of recent rule-of-law developments in Poland (as far as they relate to European law) since the last update in eucrim 3/2021, 135–137.

■ 27 October 2021: The Vice-President of the CJEU orders Poland to pay the Commission a periodic penalty payment of € 1 million per day since the country has not complied with the interim measures ordered on 14 July 2021 in Case C-204/21 (→eucrim 3/2021, 135). The reason for the penalty payment is in particular that Poland has denied so far to comply with the request to cease the exercise of the new competences by the disciplinary chamber. The Vice-President follows the Commission's application and held that "it appears necessary to strengthen the effectiveness of the interim measures imposed by the order of 14 July 2021 by providing for the imposition of a periodic penalty payment on Poland in order to deter that Member State from delaying bringing its conduct into line with that order." Poland must pay as long as the disciplinary chamber is acting; according to the CJEU, the disciplinary chamber fails to be independent and impartial. The final judgment in the dispute between the Commission and Poland will be delivered at a later stage by the CJEU's Grand Chamber.

■ 4 November 2021: The President of the CJEU, *Koen Lenaerts*, warned at the congress of the International Federation of European Law (FIDE) that the

European project in its current form is at stake. The CJEU and the primacy of EU law are currently in "an extremely serious situation". He called for the principle of the primacy of EU law to be upheld. He also recalled that membership in the EU is voluntary and is exercised by democratic and sovereign decision. As long as a Member State is part of the Union, it must accept EU law and the interpretation of EU law by the CJEU. These comments were a clear hint to the judgment of the Polish Constitutional Tribunal of 7 October 2021 in which the primacy of EU law over national constitutional law was denied (→eucrim 3/2021, 137).

■ 8 November 2021: The ECtHR rules that the procedure for appointing judges to the Chamber of Extraordinary Review and Public Affairs had been unduly influenced by the legislative and executive powers. That amounted to a fundamental irregularity that adversely affected the whole process and compromised the legitimacy of the Chamber which cannot be considered an "independent and impartial tribunal established by law" within the meaning of Art. 6(1) ECHR. The ECtHR's ruling concerned applications by two judges who took legal action against decisions by the National Council of the Judiciary (NCJ) on their applications for judicial posts (application nos. 49868/19 and 57511/19, *Dolińska-Ficek and Ozimek v Poland*). With respect to the appointment procedure of the NCJ, which deprives the Polish judiciary of the right to elect judicial members of the NCJ and enables the Polish executive and legislature to directly and indirectly interfere, the ECtHR requests Poland to rapidly remedy the situation (Art. 46 ECHR).

■ 9 November 2021: It is reported that a judge from the Elbląg District Court is suspended since he tried to implement the CJEU's interim order of 14 July 2021 in a specific case. The judge found that the Polish Disciplinary Chamber is illegal and thus the waiver of a prosecutor's immunity was not effective.

■ 16 November 2021: The CJEU declares another feature of the Polish judicial system incompatible with EU law. According to the CJEU, the Polish regulations allow the Polish Minister of Justice – who is also the Public Prosecutor General – to second judges to higher criminal courts and to terminate the secondments at any time without stating reasons, is contrary to Art. 19(1) TEU and Directive 2016/343 on the presumption of innocence in criminal proceedings. The cases were referred to the CJEU by the Regional Court of Warsaw before which the composition of the panel adjudicating several criminal cases was put into question (Joined Cases C-748/19 and C-754/19, *WB and Others*). The CJEU confirms that the secondment of a judge by the Polish Minister of Justice to the court jeopardizes the requirement of independence.

■ 24 November 2021: The Polish Constitutional Tribunal rules that Art. 6 ECHR, which guarantees a fair trial before an independent court, is not compatible with the Polish Constitution insofar as it concerns the Polish Constitutional Tribunal as a court. It is argued that the Polish Constitutional Tribunal adjudicates the hierarchy of norms and not individual complaints. The Polish Constitutional Tribunal deduces from this that Poland is not bound by ECtHR decisions which concern the Tribunal itself. The decision is a reaction to the ECtHR's decision of 7 May 2021 in the case *Xero Flor* (→eucrim 2/2021, 71), in which the judges in Strasbourg found that the election of judges to the Polish Constitutional Tribunal in 2015 was irregular and thus infringed the applicant's rights to a "tribunal established by law" in accordance with Art. 6(1) ECHR.

■ 15 December 2021: MEPs debate on the latest worrying developments in Poland. This includes the decision by the Polish Constitutional Tribunal of 24 November 2021 on the partial incompatibility of Art. 6 ECHR with the Polish Constitution (cf. above), the de facto ban on abortion, the issue of "LGBTIQ-free zones" (→eucrim 3/2020, 161), and the slow progress in the Article 7 procedure against Poland. MEPs call on the Council, the Member States and the Commission to step up their efforts to stop the continuous deterioration of EU values in Poland.

Hungary: Rule-of-Law Developments November to December 2021

This news item continues updates on recent rule-of-law developments in Hungary (as far as they relate to European law). For the last overview →eucrim 3/2021, 137–138.

■ 16 November 2021: In the infringement proceedings between the Commission and Hungary on the Hungarian asylum legislation (Case C-821/19), the CJEU follows the Advocate Generals opinion of 25 February 2021 (→eucrim 1/2021, 5) and holds that Hungarian law which criminalises the organising activity of persons for international protection of asylum seekers in Hungary infringes EU law. The CJEU found that the Hungarian legislation restricts, first, the right of access to applicants for international protection and the right to communicate with those persons and, second, the effectiveness of the right afforded to asylum seekers to be able to consult, at their own expense, a legal adviser or other counsellor. In sum, criminalising such activities impinges on the exercise of the rights safeguarded by the EU legislature in respect of the assistance of applicants for international protection.

■ 23 November 2021: The CJEU rules on the handling of a reference for a preliminary ruling by the Hungarian judiciary (Case C-564/19). The background is a criminal case in Hungary against a Swedish citizen who was assisted by an interpreter during the first interrogation. The competent judge in Hungary had doubts about the selection and skills of the interpreter. In this context, he referred questions to the CJEU for a preliminary ruling as regards the interpretation of Directives 2010/64 and

2012/13 (guaranteeing rights to translation/interpretation and information in criminal proceedings). At the request of the Hungarian Prosecutor General, the Hungarian Supreme Court declared the request for a preliminary ruling unlawful. Disciplinary proceedings were initiated against the judge as well. The CJEU now rules that the review of the request for a preliminary ruling was contrary to EU law. The CJEU has exclusive jurisdiction to review the admissibility of requests for a preliminary ruling. In addition, the initiation of disciplinary proceedings against the national judge also violates EU law. This impairs the mechanism of preliminary references and judicial independence. It also jeopardised the uniform application of EU law. For the question in substance, the CJEU emphasised the right of every accused person to be informed of the charges against him in a language he understands. Member States must take specific measures to ensure this right. A register of certified interpreters could help. Furthermore, the measures adopted by the Member States must enable the national courts to ascertain that the interpretation was of sufficient quality, so that the fairness of the proceedings and the exercise of the rights of the defence are safeguarded. If the national judge considers the interpretation provided inadequate or he/she cannot ascertain its quality, criminal proceedings conducted *in absentia* may be discontinued because the rights of defence are infringed.

■ 8 December 2021: In a joint letter ahead of the General Affairs Council meeting on 14 December 2021, several NGOs urge the Council to take essential steps in the Article 7 procedures against Poland and Hungary. The NGOs voice their concern over "the bold defiance of the authority of the CJEU and the ECtHR by the governments of both Poland and Hungary". They also demonstrate that the governments of Hungary and Poland have continued on their path away from the founding EU values despite numerous efforts made by the EU institutions.

■ 10 December 2021: The Hungarian Constitutional Court decides on a motion of Hungarian Minister of Justice *Judit Varga,* which asked the Court whether Hungary does not need to follow the important CJEU judgment of 17 December 2020, by which the Hungarian procedure for granting international protection and returning illegally staying third-country nationals were declared incompatible with EU law. On the one hand, the Hungarian Constitutional Court emphasized that it is not in the position to review specific CJEU judgments. Observers assess this as the failure of the Minister's attempt to get a *carte blanche* to ignore the CJEU's binding judgment as did the Polish Constitutional Court (→eucrim 3/2021, 137). As a consequence, Hungary would in particular be obliged to stop its practice of push-backs at its borders. On the other hand, the Hungarian Constitutional Court held that "where the joint exercise of competences is incomplete, Hungary shall be entitled, in accordance with the presumption of reserved sovereignty, to exercise the relevant non-exclusive field of competence of the EU, until the institutions of the European Union take the measures necessary to ensure the effectiveness of the joint exercise of competences". This can be interpreted that Hungary has the sovereign right to pass laws for the protection of fundamental rights – until the conditions to effectively execute EU law are guaranteed. Furthermore, the Hungarian Constitutional Court draws conclusions from the "right to self-determination stemming from one's traditional social environment". This could mean that Hungarians have the right to live in a more or less homogeneous country, where people are not too different from one another.

■ 31 December 2021: The Hungarian Helsinki Committee publishes a research paper in which it is demonstrated that Hungary has been failing to implement judgments of the Strasbourg and Luxembourg courts, and Hungarian authorities are repeatedly disregarding the judgments of the country's own domestic courts. This is seen as another sign of the country's rule-of-law backsliding. (TW)

EP Observes Rule-of-Law Deterioration in Slovenia

On 16 December 2021, the European Parliament adopted (with 356 votes for, 284 against, and 40 abstentions) a resolution on the situation of fundamental rights and rule of law in Slovenia. Despite positive developments, the resolution tackles several threats to democracy and media freedom in Slovenia. These include media defunding, online harassment, strategic legal actions (SLAPPs), threats against critical voices, the delayed appointment of delegated prosecutors to the EPPO, delayed appointments of state prosecutors to relevant investigations, the proliferation of illiberal political movements, and corruption. MEPs call on the Slovenian government to adopt or implement the underlying EU rules and guarantee that the common European values listed in Art. 2 TEU are upheld in full.

The resolution concludes a plenary debate on the rule of law situation in Slovenia in November 2021 and a mission of an EP delegation that travelled to Slovenia in October 2021 to assess respect of EU values with national authorities, journalists and NGOs. (TW)

CJEU: Exclusion of Blind Juror from Participating in Criminal Proceedings Not Justified

On 21 October 2021, the CJEU ruled that a blind person cannot be deprived of his/her possibility to perform the duties of a juror in criminal proceedings. The case at issue (C-824/19) plays in Bulgaria, where a woman, VA, who has a permanently reduced capacity to work due to loss of vision, had studied law and been admitted as a juror by the *Sofiyski gradski sad* (Sofia City Court, Bulgaria). She was assigned to a criminal chamber of that court but did not participate in a single oral procedure in criminal pro-

ceedings in the period from 25 March 2015 to 9 August 2016.

The CJEU had to decide whether the exclusion of a blind person from performing duties as a juror in criminal proceedings was compatible with the provisions of Directive 2000/78 establishing a general framework for equal treatment in employment and occupation, read in light of the guarantees of non-discrimination enshrined in the EU Charter of Fundamental Rights (CFR) and the UN Convention on the Rights of Persons with Disabilities. The CJEU noted that VA had been excluded from all participation in criminal proceedings, irrespective of the matters concerned and without any effort to determine whether reasonable accommodation could be provided. The CJEU also observed that, after the introduction of electronic allocation of jurors in August 2016, VA participated as a juror in the judgment of numerous criminal matters. Therefore Art. 2(2)(a) and Art. 4(1) of Directive 2000/78, read in the light of Arts. 21 and 26 of the CFR and of the UN Convention, must be interpreted as meaning that they preclude depriving a blind person of the possibility of performing the duties of a juror in criminal proceedings. (AP)

Schengen

Updated Rules Reinforcing Governance of Schengen Area

On 14 December 2021, the Commission proposed updated rules to reinforce the governance of the Schengen area. The Commission stressed that the Schengen area is one of the biggest achievements of European integration. It has been repeatedly put to the test in recent years by a series of crises and challenges (e.g. the refugee crisis and the COVID-19 pandemic). While the already existing framework provides tools to tackle such challenges, there is room for improvement of certain aspects (e.g. dealing with major public health threats and the instrumentalisation of migrants). Therefore, the Commission sees the need to stock up the range of tools available to ensure the proper functioning of the Schengen area in order to restore and reinforce mutual trust between Member States. The main aims of the proposal are:

- Uniform application of measures at the external borders in case of a threat to public health: in such cases, the Council should be allowed to quickly adopt binding rules on temporary travel restrictions.
- Response to instrumentalisation of migrants at external borders to address the situation where a third-country actor uses human beings to destabilise the Union or its Member States: The proposal suggests provisions that will allow Member States to take the measures needed to manage the arrival of persons being instrumentalised by a third country. The measures will respond to the situation in a humane, orderly, and dignified manner that is fully respectful of fundamental rights and humanitarian principles.
- Contingency planning for Schengen in a threat situation affecting a majority of Member States at the same time: The proposal clarified and expanded the list of elements that must be assessed by a Member State when reintroducing temporary border controls. The Member State must review the appropriateness of the measure and its likely impact on the movement of persons within the Schengen area (without internal border control) and on the cross-border regions. The possibility to extend border controls up to a total maximum period of two years if certain threats persist for a considerable amount of time has also been added.
- Increased use of alternative measures to address the identified threats instead of internal border controls.

The Commission's proposal to revise the Schengen Borders Code is part of other measures that aim to improve Schengen's overall functioning and governance under the new Schengen Strategy "Towards a stronger and more resilient Schengen area" (→eucrim 2/2021, 76). (AP)

OSCE Makes Recommendations on Use of New Technologies for Border Management

On 5 October 2021, the Organization for Security and Co-operation in Europe (OSCE) released a new policy brief on Border Management and Human Rights. The policy brief aims at providing an overview of the what the implications of collecting and sharing information in the context of border management are and how the introduction or continued use of new technologies in the border space may affect human rights. It also provides recommendations to OSCE-participating States on how to respect and protect human rights when using new technologies to manage their borders.

The brief calls to mind that, while states have a legitimate interest in controlling their borders and managing who enters their territory, border security must not come at the expense of human rights and fundamental freedoms. It is therefore necessary to put in place a robust legislative framework that both regulates the use of new technologies at borders and provides strong human rights safeguards.

The OSCE points out that the collection and automated processing of Advance Passenger Information (API) and Passenger Name Records (PNR) data by state authorities (via airlines) is a substantial interference with the right to privacy. Therefore, states need to clearly and convincingly demonstrate how the use of this data is limited to what is strictly needed in order to achieve a legitimate aim, such as the prevention, detection, and investigation of terrorist offences or other serious crimes. Furthermore, states need to minimize the amount of data being collected and minimize data retention periods. They should also strictly observe purpose limitations for data processing. The collection and

processing of sensitive data like PNR should not be permitted.

As API and PNR data are used to identify terrorist suspects among travellers by means of comparison with relevant watchlists and databases, there can be wrongful identification that can impact freedom of movement. PNR data is also used for a general data analysis of the traveller as well as specific risk assessments of behaviour to detect potential suspicious patterns. This can lead to discriminatory profiling. Therefore, states need to put in place effective human rights safeguards to protect persons from being placed under wrongful suspicion for involvement in terrorism or other crimes, and states must refrain from discriminatory profiling on the basis of PNR data.

Regarding biometric data systems, the OSCE stressed that all systems operating with biometric data should be presumed high-risk technologies. They should undergo thorough and independent human rights impact assessments. States must also put in place clear human rights-based frameworks, which strictly regulate the use of biometric technology.

Especially refugees, asylum-seekers, and children crossing borders are at particular risk of human rights violations arising from the use of biometric data. In these cases, alongside privacy and data protection concerns, there are particular risks of infringements of absolute rights (the risk of refoulement; cruel, inhuman, and degrading treatment; or other infringements on human dignity). For persons in situations of heightened vulnerability, such as migrants and asylum-seekers, states must ensure that the principle of free and informed consent and the right to information are guaranteed whenever collection and processing of biometric data (e.g. fingerprints) takes place. For asylum seekers, the states should follow the well-established principle of not sharing the biometric data of asylum seeker with the country of origin. The OSCE sees a high risk in the use of biometric technology, such as facial recognition, which may reinforce bias and result in discrimination; the organization urges states to reconsider the use of such technology.

Regarding the use of algorithms, the OSCE points out that the technology is not a neutral technical tool that helps screen individuals and inform consequent decision-making in border control, since there is a risk of introducing bias to the algorithm through biased data sets. Therefore, algorithmic systems should undergo obligatory and regular audits in addition to "discrimination testing" by private companies as well as public bodies involved in the development and operation of such systems. Border guards working with such tools should also receive human rights and anti-discrimination training. It is also imperative that algorithmic decision-making tools remain under human control.

In order to avoid overbroad application of terrorism watchlists, the criteria for including individuals on such lists must be clearly defined, based on a narrow and precise definition of terrorist offences. Human rights safeguards must be integrated into all terrorism-related international and transnational co-operation agreements, including in relation to data sharing. (AP)

Legislation

Proposals to Modernise EU Cross-Border Judicial Cooperation via Digitalisation

spot light

On 1 December 2021, the Commission adopted two proposals to improve the digitalisation of cross-border judicial cooperation:

- Proposal for a Regulation laying down rules on digital communication in judicial cooperation procedures in civil, commercial and criminal matters;
- Proposal for a Directive aligning the existing rules on communication with the rules of the proposed Regulation.

The Commission acknowledged that most data exchanges in cross-border judicial cooperation to date are still paper-based. By means of this digitalisation initiative, the Commission aims to increase the efficiency and resilience of EU cross-border judicial cooperation through enhanced digitalisation in civil (including family), commercial, and criminal matters. The Commission further intends to improve access to justice for citizens and businesses. The new legislation therefore makes mandatory the use of a digital channel for all Union-wide, cross-border judicial cooperation communication and data exchanges between the competent national authorities.

By using national IT portals, or a European Access point hosted on the European e-Justice Portal, citizens and businesses will have the opportunity to communicate with courts and other judicial authorities of the Member States electronically using a qualified or advanced electronic signatures and/or seals. Judicial fees will be payable electronically.

Under certain conditions, the new legislation will make oral hearings able to be held remotely using videoconferencing, in both civil and criminal cases. It comes along with a proposal on a better digital information exchange in terrorism cases and a proposal for the establishment of a special IT platform to support the functioning of Joint Investigation Teams (→following two news items). For details on this digitalisation initiative, see also the contribution by the EU Commissioner for Justice *Didier Reynders*, p. 236 of this issue. (AP)

Proposal to Improve Digital Information Exchange in Terrorism Cases

On 1 December 2021, the European Commission launched a new initiative to digitalise EU justice systems and to improve digital information exchange in terrorism cases. The main goal of this proposal is to render the exchange of information between the competent

national authorities, Eurojust, and the European Judicial Terrorism Register more efficient.

The proposal aims to establish secure digital communication channels between Member States' competent national authorities and Eurojust in order to ensure the swift and secure exchange of information. The regulation will also enable Eurojust to crosscheck information effectively by identifying links between prior and ongoing cross-border terrorism cases and other types of serious cross-border crime. The identification of such links will enable Member States to better coordinate their investigation measures and judicial responses. (AP)

Proposal for JIT Collaboration Platform

On 1 December 2021, the European Commission adopted a new initiative establishing a collaboration platform to support the functioning of Joint Investigation Teams (JITs). The Commission noted that JITs, which are set up by two or more States for specific criminal investigations with a cross-border impact and for a limited period of time, have been experiencing a number of technical difficulties rendering them less efficient. One specific problem concerns how to ensure the secure electronic exchange of information and evidence and secure electronic communication with other JIT members and JIT participants (such as Eurojust, Europol, and the European Anti-Fraud Office (OLAF)).

In order to solve these issues, the Commission proposes the establishment of a dedicated IT platform to support the functioning of JITs, which will be accessible to all actors involved in JIT proceedings and have the following features:

- A secure, untraceable communication stored locally on the devices of the users, including a communication tool offering an instant messaging system, a chat feature, audio-/videoconferencing, and a function replacing standard emails;
- An upload/download system designed to ensure the efficient exchange of information and evidence, including large files – it will store the data centrally only for the limited time needed to technically transfer the data;
- An advanced logging mechanism to track the trail of "who did what and when" for all evidence shared through the platform, in this way supporting the need to ensure the admissibility of evidence before a court.

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) will be in charge of the design, development, technical management, and maintenance of the JIT collaboration platform. The proposal on the JIT collaboration platform is part of a larger package on the digitalisation of justice. For the other initiatives, see also the contribution by EU Commissioner for Justice, *Didier Reynders*, p. 236 of this issue. (AP)

European Council's Conclusion on Digitalisation

At the summit on 22 October 2021, EU leaders discussed the EU's digital transition and adopted conclusions on the EU's digital policy in the forthcoming years. The European Council called for a swift examination of the Commission's proposal for the policy programme "Path to the Digital Decade", with a view to implementing the 2030 Digital Compass.

The European Council also reviewed the progress made on a series of key legislative files. It encouraged the Council and the EP to reach an agreement on the Roaming Regulation, the Digital Services Act, and the Digital Markets Act as soon as possible. Furthermore, the need to make headway in the following areas was stressed:

- Implementing the remaining measures necessary to establish specific sectoral data spaces, as set out in the European strategy for data of February 2020, and establishing a roadmap for this process;
- Establishing an innovation-friendly regulatory framework for artificial intelligence in order to accelerate the uptake of this technology while safeguarding fundamental rights;
- Setting common standards for and agreeing on a coordinated approach towards a European Digital Identity framework;
- Promoting the creation of a cutting-edge European microchip ecosystem.

In order to tackle the problem of an increase in malicious cyber activities, the European Council called for accelerated work on the proposal for a revised Directive on Security of Network and Information Systems, the proposed Directive on the Resilience of Critical Entities, and the Cyber Diplomacy Toolbox (→eucrim 4/2020, 282–283). (AP)

Civil Society Organisations Call for Prioritisation of Fundamental Rights in Artificial Intelligence Act

On 30 November 2021, 115 civil society organisations published a collective statement calling for EU institutions to prioritise fundamental rights in the Artificial Intelligence Act (AIA). The statement outlines recommendations to guide the European Parliament and Council of the European Union in amending the European Commission's AIA proposal (→eucrim 2/2021, 77). In their statement, the civil society organisations voice several demands, including the following:

- A cohesive, flexible, and future-proof approach to the "risk" of AI systems: The statement calls the AIA's current risk-based approach dysfunctional. The *ex-ante* approach of designating AI systems to different risk categories does not take into consideration that the level of risk also depends on the context in which a system is deployed, which cannot be fully determined in advance. Hence, robust and consistent update mechanisms for "unacceptable" and limited-risk AI systems should be introduced;
- Prohibitions on all AI systems posing an unacceptable risk to fundamental

rights: The scope of Art. 5 of the AIA should be expanded to include social scoring systems, remote biometric identification in public places, emotion recognition systems, discriminatory biometric categorisation, AI physiognomy, and systems used to "predict" criminality or to profile and risk-assess in the context of immigration control;

- Obligations on users of high-risk AI systems to facilitate accountability towards those impacted by AI systems: this includes the obligation to conduct a fundamental rights impact assessment (FRIA) before deploying any high-risk AI system;
- Consistent and meaningful public transparency;
- Meaningful rights and redress for persons impacted by AI systems;
- The introduction of horizontal, public-facing transparency requirements on the resource consumption and greenhouse gas emission impacts of AI systems;
- Improved and future-proof standards for AI systems;
- A truly comprehensive AIA that works for everyone by ensuring data protection and privacy for persons with disabilities. (AP)

DAV Position Paper on Commission's Artificial Intelligence Act Proposal

On 25 November 2021, the German Bar Association (Deutscher Anwaltverein – DAV) published a position paper on the Proposal of the European Commission for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, adopted on 21 April 2021 (COM(2021) 206 final) (on the Commission's Proposal →eucrim 2/2021). The DAV welcomed the risk-based approach of the AIA Proposal but points out that the binary classification into high-risk/non-high-risk AI systems leaves less room for differentiation of other risk levels.The association welcomed the EU Commission's proposal but criticised the definition of AI systems in Art. 3(1) of the proposal as being too narrow with regard to future developments, as it refers to human-defined objectives. It does not object to Art. 5 of the proposal's lists of intolerable and prohibited AI systems. However, the DAV advocates clear criteria that would help distinguish between AI systems that are prohibited and AI systems that are permitted.

The DAV further welcomed the prohibition of social scoring but expressed regret that the prohibition has been softened by the conditions mentioned in (i) and (ii). It sees room for broad interpretation in the wording of the conditions (e.g. terms such as "unrelated to the contexts" (i) or "unjustified or disproportionate" (ii)).

The association criticizes that only biometric identifications in real time-situations have been banned and that Art. 5 of the proposal only prohibits biometric identification systems when used for law enforcement purposes. The DAV regrets the absence of a general ban on AI systems that take independent judicial decisions, a "predictive policing" ban, and a complete ban of polygraphs. It joins the CCBE Position Paper in its call for a ban on AI systems in the areas of migration, asylum, and border control management until they have been independently assessed for compliance with international human rights standards.

With regard to use of AI in the area of law enforcement, the DAV stressed that, in cases in which decisions are based on data or results are produced by an AI system, the parties and/or their lawyers must be able to access this AI system in order to assess its characteristics, the data used, and the relevance of the results it provides. For the use of AI in the justice area, the association recommends that detailed principles and guidelines be established and that AI systems only be introduced if sufficient safeguards against discrimination and bias are in place. (AP)

Institutions

Council

Programme of the French Council Presidency

On 1 January 2022, France took over the Presidency of the Council of the European Union for six months. This is also the first Presidency in the new cycle of trio presidencies composed of France, the Czech Republic, and Sweden (→following news item).

Under the title "Recovery, Strength and a Sense of Belonging," the programme of the French Presidency is guided by three objectives:

- To build a more sovereign Europe;
- To create a new European model for growth;
- To form a humane Europe.

In the area of Justice and Home Affairs, the programme strives to move forward with the reform of the Schengen area, to continue working on asylum and migration, and to strengthen security for European citizens. As part of the latter objective, the programme suggests strengthening police cooperation in the EU. In this regard, the Presidency plans to further promote the police cooperation package (→news item, p. 225) by doing the following:

- Continuing negotiations to revise the Europol Regulation;
- Enhancing information exchange between European police forces;
- Establishing a directive on information exchange between law enforcement authorities of the EU Member States.

Additional efforts will be taken to step up the fight against drug trafficking and to combat terrorism and radicalisation, especially with regard to the return of foreign terrorist fighters and the detection of terrorist individuals in the Schengen area. The idea of creating an "EU Knowledge Hub" for the prevention of radicalisation will be further promoted. Looking at legal instruments, the French Presidency intends to strengthen its efforts against online child sexual

abuse and to carry out negotiations on the upcoming proposal of the European Commission on preventing and combatting the sexual abuse of minors. (CR)

Programme of New Trio Council Presidencies

spot light

31 December 2021 marked the end of a cycle of trio presidencies. The cycle had started with the German Presidency on 1 July 2020 (→news of 31 August 2020), continued with the Portuguese Presidency on 1 January 2021 (→news of 1 April 2021), and the Slovenian Presidency took over on 1 July 2021 (→news of 6 July 2021).

On 1 January 2022, a new trio of presidencies of the Council of the EU started its work. Between now and 30 June 2023, the rotating presidency will be held by France, the Czech Republic, and Sweden, in turn – each term being six months long.

The trio's programme sets out a series of thematic priorities:

- To protect citizens and freedoms;
- To promote a new growth and investment model for Europe;
- To build a greener and more socially equitable as well as more global Europe.

In the area of police and judicial cooperation, the three Presidencies pursue the following objectives:

- Strengthening the Schengen area as a space of free movement without internal borders;
- Enhancing the effective protection of Schengen's external borders;
- Reinforcing the Schengen evaluation mechanism and improving its governance;
- Combating organised crime, chiefly human, drugs, and arms trafficking;
- Fighting all forms of terrorism, radicalisation, and violent extremism as well as environmental crime;
- Making greater efforts to better protect victims of terrorism.

The trio also intends to address issues in the field of money laundering and asset recovery as well as the prevention of crimes against cultural heritage. Other priorities include:

- The disruption and identification of high-risk criminal networks active in the EU;
- The deployment and interoperability of EU information systems;
- The strengthening of e-justice and the continued development of digital information exchanges between judicial authorities.

Looking at legislative measures, the trio aims to find an agreement on e-evidence legislation and plans to work on a proposal for a new legal instrument on the transfer of proceedings. (CR)

European Commission

Commission Work Programme 2022

On 19 October 2021, the European Commission published its new Work Programme 2022, setting out its key initiatives for the year ahead. A major feature of the Work Programme 2022 is the so-called "one-in, one-out" approach, aiming to reduce the burdens placed on citizens and businesses in the same policy area whenever new initiatives are introduced.

Under the title "Making Europe stronger together", the Work Programme contains new legislative initiatives across all six headline ambitions, namely:

- A European Green Deal;
- A Europe Fit for the Digital Age;
- An Economy that Works for People;
- A Stronger Europe in the World;
- Promoting our European Way of Life;
- A New Push for European Democracy.

In the area of Justice and Home Affairs, the Work Programme foresees new (legislative) initiatives in the following areas:

- Security and defence technologies;
- Cyber resilience;
- Advance passenger information;
- Reciprocal access to security-related information between the EU and key third countries;
- Transfer of criminal proceedings.

Furthermore, the Commission plans to assess how to achieve convergence on pre-trial detention and detention conditions between Member States as part of improving cross-border cooperation in criminal matters. Lastly, the Commission will continue its work on the relevant legislative files regarding a future-proof security environment, in order to tackle evolving threats, to protect Europeans from terrorism and organised crime, and to develop a strong and secure European ecosystem. The Work Programme is supplemented by an Annex listing the new initiatives and envisaged repeals. (CR)

New Tripartite Agreement Allowing the ECA to Have More Access to EIB Data

On 11 November 2021, the European Court of Auditors (ECA), the European Investment Bank (EIB), and the European Commission signed a new tripartite agreement. It replaces an agreement from 2016 that was concluded between these three institutions. The revised tripartite agreement allows the ECA wider access to EIB documents and data relating to activities carried out under the mandate of the European Commission. The agreement further clarifies the timeline for receiving necessary audit documentation (and in what format), confidentiality, data protection rules, evidence collection methods, and access to information. (AP)

European Court of Justice

Personnel Changes at the CJEU

The terms of office of 14 judges and six advocates general of the Court of Justice of the EU expired on 6 October 2021 and the terms of office of 23 judges of the General Court expired on 31 August 2021. In October 2021, a series of personnel changes took place at the EU Court of Justice and the General Court. The nominations are part of the partial renewal of their composition.

■ For the Court of Justice of the EU, Mr *Koen Lenaerts* was re-elected to serve as its President from 8 October 2021 to 6 October 2024. Mr *Lars Bay Larsen* was elected Vice President of the Court of Justice from 8 October 2021 to 6 October 2024. He succeeds Ms *Rosario Silva de Lapuerta*. Mr *Maciej Szpunar* was elected First Advocate General of the Court of Justice for the period from 8 October 2021 to 6 October 2024. Lastly, Mr *Siniša Rodin*, Mr *Irmantas Jarukaitis,* Mr *Niilo Jääskinen*, Ms *Ineta Ziemele*, and Mr *Jan Passer* were elected Presidents of the Chambers of three judges for a period of one year.

■ For the period from 7 October 2021 to 6 October 2027, the terms of office of the following seven judges of the Court of Justice were renewed: Mr *Koen Lenaerts*, Mr *Lars Bay Larsen*, Mr *Siniša Rodin*, Mr *François Biltgen*, Mr *Eugene Regan*, Mr *Niilo Jääskinen*, and Ms *Küllike Jürimäe*.

■ For the same period, the following five new judges of the Court of Justice started their terms of office: Ms *Maria Lourdes Arastey Sahún*, Mr *Zoltán Csehi*, Ms *Octavia Spineanu-Matei*, Mr *Miroslav Gavalec*, and Mr *Dimitrios Gratsias*.

■ From 7 October 2021 to 6 October 2027, Ms *Laila Medina*, Mr *Nicholas Emiliou*, and Ms *Tamara Ćapeta* will serve as Advocates General of the Court of Justice. In addition, for the period from 7 October 2021 to 6 October 2024, Mr *Anthony Collins* – former judge at the General Court– will serve as Advocate General of the Court of Justice; he replaces AG *Gerard Hogan*. Before joining the Court, Ms *Medina* held the position of Deputy State Secretary for Legal Policy at the Latvian Ministry of Justice. She is taking over from Mr *Henrik Saugmandsgaard Øe*. Mr *Emiliou* was Permanent Representative of the Republic of Cyprus to the EU, he succeeds AG *Michal Bobek*. Ms *Ćapeta* looks back on a longstanding academic career with the University of Zagreb and is a founding member the *Jean Monnet* Centre of Excellence for which she had served as its coordinator from 2018 to 2021. She replaces AG *Evgeni Tanchev*.

■ With regard to the General Court, Mr *Krisztián Kecsmár* (Hungary) and Mr *Ion Gâlea* (Romania) were appointed as judges from 7 October 2021 until 31 August 2022. Furthermore, for the period from 10 September 2021 to 31 August 2025, Mr *Pēteris Zilgalvis* (former Head of Unit at the European Commission) will be judge of the General Court. (CR)

OLAF

CJEU Rules on Guarantees in OLAF's External Investigations (Case *Vialto*)

spot light

On 28 October 2021, the CJEU ruled in an appeal judgment (Case C-650/19 P) on the right to be heard in administrative proceedings involving several authorities. The case concerned the Hungarian company *Vialto,* which was part of a consortium that carried out an agriculture project funded by the EU's Instrument for Pre-Accession Assistance (IPA). After an investigation of alleged corruption and fraud by OLAF, the competent Directorate General for Enlargement of the European Commission advised the national authority, which managed the funds, to exclude *Vialto* from the contract in question. *Vialto's* appeal against the judgment of the General Court of 26 June 2019 (Case T-617/17) was successful in so far as the Commission's Directorate did not confer an opportunity to be heard to the appellant before it sent a letter to the national management authority in which it informed about the breach of obligations by the company at issue and recommended to take appropriate measures.

The CJEU emphasised the importance of the right to be heard as part of the right to good administration (Art. 41(2a) CFR) and as general principle of Union law. That principle requires that the addressees of decisions which significantly affect the interests of those addressees should be placed in a position in which they may effectively make known their views with regard to the evidence on which those decisions are based. Although the final decision on appropriate measures against a beneficiary of EU funds is taken by the national authority in programmes of decentralised management, the Commission's intervention was an important – perhaps even a decisive – step in this process. Therefore, it must be maintained that the intervention is liable to affect the interests of the person/undertaking concerned and he/she/it must be heard by that Union institution, body or agency. The hearing can also not be replaced by the fact that the person/undertaking concerned was heard by OLAF during its investigations because the role of OLAF is only to submit non-binding recommendations to the competent Commission service.

Other grounds for appeal were, however, rejected by the CJEU. They concerned important questions in relation to the way in which OLAF carries out external investigations and, more specifically, the limits of digital forensic operations. In addition, the case raised issues regarding the impact of commitments given by OLAF at the beginning of an on-the-spot check in the light of the principle of legitimate expectations. In particular, the CJEU backed the interpretation by the General Court that Art. 7(1) of Regulation 2185/96 covers the possibility that OLAF makes a "digital forensic image" of a company's data for the purpose of a subsequent sifting of relevant data for the investigation in question. The Court emphasised that such digital forensic images do not mean a copying of all data sets and media owned by a controlled company, but are only an intermediate step for further sifting operations of the relevant documents.

Lastly, the CJEU ruled that an undertaking cannot rely on the principle of the protection of legitimate expectations, if it refuses to cooperate with OLAF and therefore does no longer want to follow

a proposed derogating practice in its favour in the framework of on-the-spot checks pursuant to Art. 7 of Regulation 2185/96. (TW)

New Edition of Global Operation against Medicine Trafficking

On 14 December 2021, Europol and OLAF informed the public of the second edition of operation "SHIELD" that was carried out between April and mid-October 2021 (for the first edition →eucrim news of 20 January 2021). Operation SHIELD II targeted criminal groups that traffic in misused or counterfeit doping substances and medicines, e.g. COVID-19 vaccines, anti-cancer drugs, erectile dysfunction medicines, pseudoephedrines, painkillers, antioestrogens, antivirals, etc. The operation was led by Europol and the French, Hellenic, and Italian police forces. It involved 20 EU Member States, seven non-EU countries (including Columbia and the United States), OLAF, the World Anti-Doping Agency and private companies.

Operation Shield II resulted, *inter alia*, in the seizure of 25 million units of medicines and doping substances worth nearly €63 million, the disclosure of five illegal labs, the shutdown of over 280 websites and the arrest of 544 suspects. Performance enhancing drugs and "corona-cures" were at the top of the seizures list, while the amount of COVID-19-related medicinal trafficking has significantly decreased compared to the first edition of operation Shield in 2020.

Europol supported the investigation with operational coordination and analysis. OLAF facilitated the cooperation and activities of customs and police authorities and led targeted actions. Europol's Executive Director *Catherine De Bolle*, and OLAF Director-General *Ville Itälä* stressed that it is worrying to see how criminals put people's health at risk in order to make profits. Due to close cooperation and good coordination, the EU bodies and national law enforcement authorities, however, were again successful in protecting the consumers' health, public revenues, and legitimate business, they said. (TW/CR)

OLAF Detects Major Customs and VAT Fraud with Textiles from China

On 10 November 2021, OLAF reported that it detected an EU-wide fraud scheme which damaged the EU's financial interests by €14 million of undeclared customs duties and around €93 of evaded VAT. The investigations involved a total of nearly 2000 consignments of textiles and shoes, which were imported from China through various ports in the EU by UK companies. The fraudsters underdeclared the value and they evaded VAT through various shipments in the EU. Goods disappeared from official customs controls and were likely sold on the black market. The case concerned 11 EU Member States to which OLAF send recommendations for recovery. It was also reported to the EPPO for criminal follow-up investigations. (TW)

Successful Third-Country Cooperation against Smuggling of Cigarettes

On 14 October 2021, OLAF reported that the Ukrainian customs authorities successfully dismantled a cargo with over 13 million smuggled cigarettes with a weight of over 14.5 tonnes. The cigarettes were hidden in a shipment of tires. OLAF transmitted information from the Indian customs services to the Ukrainian State Customs Service about the suspicious shipment from India destined for the EU. (TW)

Operation against Illicit Trade in Refrigerant Gases

Within the framework of a joint investigation week that took place between 20 and 25 September 2021, law enforcement authorities in 16 countries cracked down on the illegal import of refrigerant gases (HFCs – hydrofluorocarbons). The operations were coordinated by Dutch authorities, OLAF and Europol. In total, 2100 cylinders of F-gases were seized and seven suspects arrested. The estimated value of the illicit trade is over €10 million. Other administrative and criminal infringements were notified. The fight against illicit HFCs is one of the priorities of OLAF's work. Often, traders try to circumvent the strict EU rules on HFCs which is commonly used for cooling units. The EU set the goal to reduce consumption and production of HFCs by 79% by 2030 (compared to levels in 2014). For other previous actions against the illicit trade in HFCs →eucrim news of 29 July 2021 and of 1 April 2020. (TW)

European Public Prosecutor's Office

EPPO Appointed EDPs from Slovenia

On 24 November 2021, the EPPO College appointed two European Delegated Prosecutors from Slovenia. The appointment seems to put an end to a dispute between the EU and Slovenia, which delayed the nomination of the country's candidates for months (→eucrim 2/2021, 82–83). The Slovenian government, however, clarified that the nomination is "temporary" only, since the EDPs must still be officially selected via the national nomination procedure. It is assumed that the government wants to leave a backdoor open if its bill for an amendment to the act on public prosecution comes into force. The amendment will give the government a greater say in the appointment of delegated prosecutors effectively diminishing the powers of the national Public Prosecutor's Council that currently takes the final decision on the nominations. In return, the EPPO stressed in its press release that the two Slovenian EDPs "have been appointed for the full period of 5 years, like all other European Delegated Prosecutors". This seemed to signal that the move by the Slovenian governments is unlikely to succeed because national governments cannot recall their delegated prosecutors, otherwise the independence of the EPPO would be prejudiced.

The appointment means that now all Member States participating in the scheme of the EPPO, which was established by enhanced cooperation, have European Delegated Prosecutors. The EPPO assumed its investigatory and prosecutorial tasks on 1 June 2021 (→special eucrim issue 1/2021). The aim is to improve the prosecution of criminal offences affecting the EU's financial interests. Hungary, Poland, Ireland, and Denmark do not participate. Sweden is expected to join the scheme in 2022. (TW)

Working Arrangement between EPPO and EIB Group

On 7 December 2021, the EPPO signed a working arrangement with the European Investment Bank and the European Investment Fund. The Arrangement lays down the rules on cooperation between the EPPO and the European Investment Bank (EIB) Group. Cooperation will mainly consist of the exchange of information (including personal data) and other cooperative activities, e.g. exchange of strategic information, trainings and staff exchanges. Cooperation will relate to the relevant areas of crime within the mandate of the EPPO, in particular criminal offences affecting the EU's financial interests as provided for in the PIF Directive. The provisions of the Arrangement regulate, *inter alia*, the following in detail:

- The EIB Group's obligation to report suspicious criminal conduct to the EPPO;
- EPPO's access to information stored in the EIB Group's databases;
- Information relating to the exercise of competence by the EPPO;
- Precautionary measures to be taken by the EIB Group;
- Support to be provided by the EIB Group in individual cases;
- Data protection rules;
- Waiver of immunity and inviolability of premises, buildings, and archives of the EIB Group.

The Working Arrangement entered into force on 8 December 2021. (TW)

CCBE Concerned over Defence Rights in EPPO Proceedings

In a statement published on 10 December 2021, the Council of Bars and Law Societies of Europe (CCBE) voiced concerns over the position of the defence and procedural rights during EPPO proceedings. The CCBE identified four issues of major concern:

- Since the EPPO Regulation lacks specific provisions on defence and procedural rights, proceedings at the national level may not be fairly conducted and lack consistency;
- Since there is no regression clause, some Member States implemented the EPPO Regulation in a way that suspects do not enjoy the same rights than in purely national criminal proceedings which leads to the non-equal treatment of suspects in Member States;
- Since there are no uniform standards as regards the handling of information in the case file, the right to access to the case file is jeopardised. In particular with regard to the Content-Management-System of the EPPO, "electronic equality of arms" and "access to justice" must be ensured, e.g. by giving an effective, certified, checked and traceable digital access to all and updated materials of the case for any individual defence lawyer involved in an EPPO proceeding.
- Since the EPPO Regulation does not exclude the possibility of forum shopping (Art. 26 of Regulation 2017/1939), legal uncertainty occurs. As a minimum, the EPPO regulations should provide for a right of the accused to be heard before such a jurisdictional change, and a right for the accused to apply for a jurisdictional change. (TW)

First Conviction in EPPO Case

The EPPO reported that on 22 November 2021, the first conviction was handed down following an EPPO investigation. A criminal court in Slovakia convicted a former mayor for an attempted offence against the EU's financial interests. The mayor falsified documents in an attempt to illegally obtain money from the European Social Fund. The potential damage could have been €93,000. The court imposed a conditional imprisonment of 3 years and disqualified the mayor for a position in public office for 5 years. (TW)

EPPO and OLAF Lead Successful Investigation into Procurement Fraud in Croatia

The EPPO and OLAF conducted one of the first joint operations. The investigations concerned procurement fraud in the purchase of an information system for the Croatian Ministry of Regional Development and EU Funds (MRRFEU). The investigations resulted in the arrest of four suspects on 10 November 2021; they involved the minister of the MRRFEU, the Director of Croatia's Central Finance and Contracting Agency (SAFU), and two businessmen. The EPPO's press release described in detail the detected fraud scheme. The suspects used their positions to adjust the procurement specifications and to conduct a negotiated procurement procedure without a public tender. The total damage for the EU's financial interests is around € 1.8 million.

The case was transmitted by OLAF to the EPPO in June 2021. OLAF supported the investigations by two on-the-spot checks and digital forensic operations in Croatia. (TW)

EPPO: Operational Activities – Reports from October to December 2021

After having assumed its investigative and prosecutorial tasks in June 2021, the EPPO regularly informs the public of its operational activities. The activities reported in October/November/December 2021 include the following:

- In cooperation with the Guardia di Finanza in Sicily, the EPPO dismantled two organised criminal groups suspected of having smuggled foreign tobacco products from Tunisia to Italy. The first organisation was responsible for organising the illegal shipments from the North African coast to Italy. The sec-

ond organisation took care of retailing the goods on the market. The operation, which was carried out on 30 November 2021, led to the arrest of twelve suspects and the seizure of one speedboat, seven vehicles, and €16,000 in cash. The smuggled cigarettes had a market value of €3.5 million and caused damages of more than €6 million to the national and EU budgets.

- On 25 November 2021, the European Delegated Prosecutor in Munich, Germany coordinated an operation against aggravated customs fraud. Searches were carried out in Germany, Austria, and Slovakia against several persons who allegedly falsely declared the provenance of biodiesel and thus damaged the EU budget by more than €1.1 million.
- An operation led by the EPPO and carried out on 23 November 2021, revealed a case of corruption and money laundering in relation to the procurement process in a museum in Czechia, which is financially supported by EU funds. The Czech police seized €16,400 and conducted several house searches.
- On 18 November 2021, the EPPO targeted a beneficiary from the EU Rural Development fund in the province of Bari (Italy). The beneficiary allegedly did not modernise an *agriturismo* (farmhouse and hotel for touristic purposes), as defined in the grant agreement, but solely intended to make a profit by selling the house during the programming period. The beneficiary allegedly damaged the EU budget by €215,000.
- On 4 November 2021, the EPPO and the Guardia di Finanza in Calabria (Italy) took action against six entrepreneurs who misused EU funds. Under the EU funding scheme to promote tourism in Calabria, the suspects bought pleasure boats. However, they never used the boats for the initial, intended purpose, but moved them to Sicily where they made more profits. Assets worth €900,000 were seized.
- On 4 November 2021, an operation coordinated by the EPPO's central office in Luxembourg dismantled a criminal organisation that operated a VAT carousel fraud scheme from Germany. The scheme involved the repeated circulation of platinum coins through the same companies. Money laundering activities were also carried out in Czechia, Slovakia and Romania. Police and tax police authorities in Germany, Czechia, Slovakia and Romania arrested six suspects and seized assets worth €23 million.
- On 20 October 2021, an operation initiated by the European Delegated Prosecutor in Germany successfully stroke against Mafia organisations that had established a VAT carousel fraud scheme with luxury cars. The operation involved German, Italian, and Bulgarian authorities. 10 people were arrested and 13 luxury cars seized. It is estimated that the tax loss was around €13 million. The operation is the result of the first case that was registered with the EPPO after the body assumed its tasks on 1 June 2021. (TW)

Europol

Working Arrangement with Republic of Korea Signed

To strengthen their cooperation against serious crime, Europol and the Republic of Korea signed a Working Arrangement on 22 December 2021. It introduces a secure system for the exchange of information between the parties. Furthermore, the arrangement foresees that the parties can exchange specialist knowledge, general situation reports, and the results of strategic analysis. They can also participate in training activities and provide advice and support in individual criminal investigations. (CR)

Working Arrangement between Europol and EIB

On 29 October 2021, Europol and the European Investment Bank (EIB) signed a Working Arrangement to facilitate the sharing of information and expertise in the fight against fraud and corruption. Under the arrangement, the parties may exchange information and expertise relating to serious crime, including financial crime, e.g. money laundering, terrorism, the financing of terrorism, and cybercrime in order to better secure the financial infrastructure of the EU.

Europol: 2021 Highlights

At the end of 2021, Europol published a review highlighting its most important operations in 2021. A detailed analysis of the threat of serious and organised crime facing the EU was provided in Europol's Serious and Organised Crime Threat Assessment 2021 (→news of 2 July 2021). Last year's operations included the takedown of EMOTET, one of the most significant botnets of the last decade. "Operation Trojan Shield/Greenlight" took down the encrypted device company ANOM. In addition, the illegal use of SKY ECC-encrypted communications could be blocked. "Operation Jumita" resulted in the largest cash seizure (€16.5 m) from a criminal organisation in Spanish history. In Finland, efforts to fight terrorism resulted in the dismantling of a right-wing extremist cell. (CR)

Human Rights Organisations Oppose Europol Reform

On 21 October 2021, the European Parliament voted in favour of opening negotiations with the Council of the EU on the revision of Europol's regulation. (→news dated 10 July 2021). The vote on the Civil Liberties, Justice and Home Affairs Committee's draft report on the proposal for the revision of Europol's mandate was strongly questioned by human rights organisations. In the run-up to the vote, 25 human rights organisations, coordinated by European Digital Rights (EDRi) and including organisations such as Access Now and Statewatch, had expressed their concerns over the report's attention to the rights to fair trial, to privacy and data protection, and to non-discrimination.

In an open letter dated 20 October 2021, the organisations called on MEPs

to vote against the report. In the letter, they urged the European Parliament to include additional safeguards, e.g., mechanisms to ensure that Europol's powers are used in a proportionate way, guarantees for defence rights, and robust oversight mechanisms.

Furthermore, the organisations argue that Europol's potential new powers in the field of research and innovation contradict the core elements of the European Parliament's own resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters. Lastly, based on the claim that Europol's work largely relies on data transferred by national police authorities that contain racialised stereotypical assumptions, the organisations ask the European Parliament to wait with the expansion of Europol's mandate until the Commission's Anti-racism Action Plan 2020–2025 – which aims at improving this situation – has been duly implemented. (CR)

Eurojust

Working Arrangement between Eurojust and UK

On 20 December 2021, Eurojust and the Home Office of the UK signed a Working Arrangement to further implement the EU–UK Trade and Cooperation Agreement (TCA) that entered into force on 1 May 2021 (→eucrim 4/2020, 265–271). The Working Agreement regulates practical and administrative details regarding judicial cooperation in criminal matters between Eurojust and the UK. It sets out detailed rules with regard to the secondment of a Liaison Prosecutor to Eurojust and his/her participation in plenary meetings and working groups of the College, in operational meetings, and in coordination centres. Additionally, Eurojust may post a Liaison Magistrate to the UK. Detailed provisions regulate the exchange of information, transmission of special categories of personal data, rights of data subjects, and confidentiality. (CR)

New National Members for Cyprus and the Netherlands

In November 2021, Mr *Zacharias Symeou* took up his duties as the new National Member for Cyprus at Eurojust. Before joining Eurojust, Mr *Symeou* served as Counsel of the Republic at the Law Office of the Republic of Cyprus. As prosecutor, he litigated cases involving trafficking in human beings, murder, and trade in illicit substances.

On 3 January 2022, Mr *Alexander van Dam* started as the new National Member for the Netherlands at Eurojust. He succeeds Mr *Han Moraal* who joint Eurojust in 2014. Before his appointment at Eurojust, Mr *van Dam* worked, *inter alia*, as Resident EU Prosecutor in Belgrade, Serbia, as Acting Director of the Dutch Prosecution Service, and as Prosecutor General for the Dutch country of Aruba. (CR)

Albanian Liaison Prosecutor's Office Opens at Eurojust

On 29 October 2021, the Office of the Liaison Prosecutor for Albania opened at Eurojust, with Ms *Fatjona Memcaj* being the first Albanian Liaison Prosecutor at Eurojust (→news dated 1 April 2021).The opening of the office is one more step in implementation of the cooperation agreement signed between Albania and Eurojust in 2018 to enhance their collaboration in the fight against serious, cross-border crime (→news dated 19 January 2019). (CR)

Update of JIT Practical Guide

In December 2021, the EU Network of National Experts on Joint Investigation Teams (JITs Network) published an updated version of the JITs Practical Guide. The guide provides information in seven chapters, *inter alia*, on the following:

- Concept, operation, and setting up of JITs;
- Support offered by EU Agencies such as Eurojust, Europol, and OLAF for JITs;
- Checklist for the planning and coordination of operational activities;
- Recommendations for practical steps on how to set up a JIT.

Furthermore, the guide answers frequently asked questions, gives advice to JITs on how to receive financial support, and provides a model agreement on establishment of a JIT. Lastly, all essential tools for JIT practitioners (guidelines, forms, and templates) are listed and hyperlinked where possible. (CR)

Frontex

European Standing Corps: New Graduates

On 17 December 2021, after a six-month border and coast guard training, 109 officers from 16 EU Member States graduated as full-fledged members of the European Border and Coast Guard standing corps. The European standing corps was established to make the Schengen Area stronger and more resilient. Officers of the corps work all along the EU's external borders and in non-EU countries. (CR)

New Cooperation Plan with eu-LISA Signed

On 22 November 2021, Frontex and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) signed a renewed Cooperation Plan to further enhance their work together. The renewed Cooperation Plan runs from 2021 to 2023. The plan covers ten thematic areas, including border and migration management, IT security, research and innovation as well as personal data protection.

Currently, cooperation between the agencies focuses on the setting up of the European Travel Information and Authorisation System (ETIAS) that is being

developed by eu-LISA, with the ETIAS Central Unit hosted by Frontex (→news of 12 November 2021). (CR)

EP Agrees to Partly Freeze Frontex Budget

On 21 October 2021, the European Parliament followed the recommendation of its Budget Control Committee (→news dated 12 November 2021) and agreed to freeze part of the 2022 Frontex budget. While the European Parliament signed off on the Agency's 2019 expenses, it decided to freeze part of the 2022 budget until Frontex fulfills several conditions, such as the recruitment of 20 fundamental rights monitors and three sufficiently qualified deputy executive directors. Frontex must also set up a mechanism for reporting serious incidents at the EU's external borders as well as a functioning fundamental rights monitoring system. Of the Agency's proposed budget of €757,793,708 for the year 2022, the European Parliament decided to put €90 million in reserve (ca. 12%). (CR)

Report by Frontex Consultative Forum

On 20 October 2021, the Frontex Consultative Forum on Fundamental Rights published its Annual Report for the year 2020. The report outlines the state of play of internal and external fundamental rights safeguards at Frontex and provides recommendations on the need to further strengthen fundamental rights in Frontex' activities.

In its conclusions, the Forum requires the Agency to step up its efforts to communicate to the Fundamental Rights Officer, and to the Forum itself, to what extent their fundamental rights advice is taken into consideration in the Agency's decisions. If the advice is not taken into account, justification must be provided. Furthermore, the Forum asks for its meaningful engagement in the development and implementation of Frontex training activities. The Forum also sees the need for Frontex to establish a sound procedure within the Agency by which to launch investigations and handle allegations of fundamental rights violations. (CR)

Digitalisation of Migrant Smuggling

At the end of September 2021, Frontex and Europol finalized a joint Report dedicated to the digitalisation of migrant smuggling. The report looks at the development of digital tools and services that enable all stages of migrant smuggling, such as advertising, recruitment, communication, guidance, and payment.

So far, the tools most frequently detected in the context of migrant smuggling are commonly available apps, e.g. Facebook and WhatsApp. The report predicts the development of apps customized for migrant smuggling as the next logical step. In order to circumvent law enforcement measures, digital solutions are frequently used to conceal, lock, encrypt, delete, and modify content on devices as well as in the communication itself. The annexes to the report provide an overview of apps and platforms identified in connection with migrant smuggling. Recommendations are also made for the handling of seized mobile communication devices. (CR)

Operation "Finestra" at EU's Eastern

Between 27 September and 8 October 2021, various EU and national law enforcement agencies cracked down on transnational crime at the EU's eastern and south-eastern land borders. The joint action days code-named "Finestra" were led by Frontex and the Romanian authorities. They also involved OLAF, Europol, Eurojust, the European Border Assistance Mission to Moldova and Ukraine (EUBAM MD/UA), Interpol, and the World Customs Organization (WCO) as well as law enforcement authorities from 13 countries. The operations above all targeted smuggling of excise goods, human trafficking, and related document fraud. They resulted, *inter alia*, in the detection of 36 million illicit cigarettes, 2360 kg of tobacco, 160,000 litres of alcohol as well as 6000 litres of mineral oil; 32 smugglers were arrested. OLAF provided support through the facilitation of information exchange and checks of information against own intelligence. (TW)

Agency for Fundamental Rights (FRA)

Leaflet on Taking Fingerprints for Eurodac Translated

In 2019, FRA – in cooperation with the Eurodac Supervision Coordination Group – published a leaflet for officers and authorities on how to inform asylum applicants and migrants about the processing of their fingerprints in Eurodac in an understandable and accessible way. Since December 2021, this leaflet has been made available in almost all official EU languages and in Icelandic and Norwegian. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

Commission Proposes First Package of New Own Resources

On 22 December 2021, the Commission presented proposals to establish the next generation of own resources for the EU budget. The Commission basically relies on revenues from emissions trading, the global minimum tax for globally active companies, and a carbon border adjustment mechanism. After a start-up phase, the new revenue sources are expected to generate on average up to €17 billion per year for the EU budget between 2026 and 2030.

The new own resources will be used to redeem bonds issued by the corona reconstruction fund NextGenerationEU, which is expected to mobilise around €800 billion (in current prices) to overcome the consequences of the pandemic. The bonds issued will be redeemed by 2058 at the latest. EU leaders had agreed in July 2020 on the bond-financed

NextGenerationEU reconstruction fund guaranteeing the EU independent revenue from its own resources (→eucrim 3/2020, 174).

The Commission will now seek swift agreement on the proposed package with the European Parliament and the Council. By the end of 2023, the Commission will propose a second basket of new own resources. (TW)

CJEU Rules on Compatibility of Romanian Constitutional Court Decisions with Effective Prosecution of PIF Crimes

On 21 December 2021, the CJEU (Grand Chamber) delivered its judgment on several issues of the Romanian justice reform in the area of corruption. The referring Romanian courts mainly questioned whether several decisions of the Romanian Constitutional Court are compatible with Union law. For the cases (Joined Cases C-357/19 and 547/19 (*Euro Box Promotion and Others*) and the Joined Cases C-811/19 and 840/19 (*FQ and Others)*, the questions referred to and the Advocate General's Opinion →eucrim 1/2021, 20.

The first set of questions dealt with obligations for national legislation and national practice to ensure the effective protection of the EU's financial interests in line with Art. 325 TFEU. In this context, the CJEU reiterated its case law on the effectiveness of the protection of the EU's financial interests required by Art. 325(1) TFEU as well as Decision 2006/928 that set specific benchmarks for Romania in the areas of judicial reform and the fight against corruption. Accordingly, the Member State must not only ensure that criminal offences to the detriment of the EU's financial interests are effectively detected, investigated, and prosecuted, but also imposed penalties effectively enforced. The national legislator is obliged to ensure that there is no systemic risk of impunity, while national courts must disapply national rules that prevent the imposition of dissuasive and effective sanctions.

In the case at issue, the Romanian Constitutional Court annulled some criminal law decisions due to unlawful composition of the trial or appeal panels. According to the CJEU, this Constitutional Court case law results in the relevant fraud and corruption cases having to be re-examined, possibly several times. Given their complexity and duration, such a re-examination inevitably has the effect of prolonging the duration of the relevant criminal proceedings, which is contrary to the obligations incumbent on Romania under Decision 2006/928. Moreover, given the national statute of limitations, re-examining the cases in question could lead to the statute of limitations for the offences and prevent effective and dissuasive sanctioning of persons holding the highest offices of the Romanian state who have been convicted of committing serious fraud and/or corruption offences in the exercise of their office. This would make the risk of impunity systemic for this group of persons and would jeopardise the objective of fighting corruption at the highest level.

Regarding the consequences for defence rights, the judges in Luxembourg stated that the obligation to ensure that such offences are subject to effective and dissuasive penalties does not exempt the referring court from examining the need to respect the fundamental rights guaranteed by Art. 47 CFR. However, that court is not allowed to apply a national standard of protection of fundamental rights which would entail a systemic risk of impunity. The requirements resulting from this premise do not prevent any possible non-application of the Constitutional Court's case law on the specialisation and composition of the judicial panels in corruption cases.

A second set of referred questions concerned the consequences for national judges if they disapply the practice of the Constitutional Court. The CJEU clarified that any disciplinary liability of national judges which would be triggered for failure to comply with such judgments is contrary to judicial independence and the primacy of Union law. (TW)

AG: Regulation on Conditionality Mechanism Is Legally Sound and Compatible with EU Treaties

spot light

On 2 December 2021, Advocate General (AG) *Manuel Campos Sánchez-Bordona* recommended that the CJEU dismisses the actions brought by Hungary and Poland against the conditionality mechanism for the protection of the Union budget in the event of breaches of the principles of the rule of law (for the mechanism →eucrim 3/2020, 174–176; for the actions →eucrim 1/2021, 19). Enshrined in Regulation 2020/2092, the Council and European Parliament created a specific mechanism to ensure proper management of the Union budget where a Member State commits breaches of the rule of law which jeopardise the sound management of the European Union's funds or its financial interests. After having determined that certain rule-of-law conditions to protect the EU budget had not been fulfilled in a specific EU country, payments from the EU budget can be interrupted, reduced, terminated or suspended; new commitments can be prohibited.

The applicability of the conditionality mechanism led to disputes between the EU institutions. In particular, the European Parliament (EP) urged the Commission to apply the mechanism regardless the action by Hungary and Poland and the EP has pursued an action against the Commission for failure to act in this regard (→eucrim 3/2021, 152). Hungary and Poland had essentially based their complaints against the mechanism on the inappropriateness of the legal basis for the Regulation, a circumvention of the Article 7 TEU procedure in case of violation of fundamental values of the EU and an infringement of the principle of legal certainty (→Cases C-156/21 and C-157/21). The AG rejected all these arguments.

First, the AG concluded that Regulation 2020/2092 could correctly be based on Art. 322(1)(a) TFEU. The Regulation contains "financial rules" within the meaning of this Article and does not resemble the procedure in Art. 7 TEU. The AG mainly argued that the Regulation aims at establishing a financial conditionality instrument to safeguard the value of the rule of law of the European Union. In addition, it requests a sufficiently direct link between the breach of the rule of law and the implementation of the budget. As a result, it does not apply to all breaches of the rule of law, but only those that are directly linked to the implementation of the Union budget. The AG also pointed out that the protection of the beneficiaries of EU funds is a typical and logical measure in the shared management of those funds.

Second, the AG found that Article 7 TEU does not preclude the use of other, different instruments that protect the values enshrined in Art. 7 TEU, as is demonstrated in the CJEU's case law on the European arrest warrant and the independence of the judiciary. The AG highlighted several differences between the requirements included in Article 7 TEU and those in Regulation 2020/2092. In particular, the conditionality mechanism does not apply to all violations of the rule of law, but only to those directly related to the financial management of the Union and financial conditionality is not unusual in budgetary instruments in other areas of EU law. Hence, the AG sees no circumvention of the Article 7 TEU procedure.

Third, the AG found that the Regulation satisfies the minimum requirements of clarity, precision and foreseeability required by the principle of legal certainty. The reason is that the Regulation combines an indicative list of breaches of seven legal principles related to the rule of law with an indicative list of areas where breaches of the rule of law may arise. This demonstrated that the legislature made efforts in increasing legal certainty. (TW)

EP Sues Commission for Non-Application of the Conditionality Regulation

On 29 October 2021, the European Parliament (EP) submitted the action against the European Commission for failure to apply the Regulation on the conditionality mechanism to the CJEU. The action is registered as Case C-657/21.

Regulation 2020/2092 aims to protect the EU budget and NextGenerationEU resources from breaches of the principles of the rule of law by an EU country that adversely affect the sound financial management of the EU funds or the EU's financial interests. Based on the Regulation, payments from the EU budget can be interrupted, reduced, terminated or suspended; new commitments can be prohibited (→eucrim 3/2020, 174–176). The EP has urged the Commission to apply the Regulation against Poland and Hungary where the rule of law is under threat without waiting for a decision on the lawsuit filed by Hungary and Poland to the CJEU which seeks the annulment of the Regulation (→eucrim 3/2021, 152).

After the European Council meeting of 21/22 October 2021, Commission President *Ursula von der Leyen* confirmed that the Commission will wait for the CJEU's decision about the complaints put forward by Hungary and Poland. However, on 19 November 2021, the Commission sent "letters" to Poland and Hungary requesting information about certain rule-of-law developments in the countries. According to media reports, Poland was asked questions on the independence of the judiciary. Questions to Hungary dealt with public procurement, corruption and risks of conflict of interest. It was stressed that the letters had not formally triggered the conditionality mechanism, but the Commission expects replies that would "feed into the Commission's assessment" on how to proceed further in the application of the conditionality tool. The initiative can also be seen as a reaction to continuous criticism about the Commission's stalling tactics. It came short before the Advocate General delivered its opinion on 2 December 2021, in which he assessed the actions brought by Hungary and Poland against the conditionality mechanism (→aforementioned news item). (TW)

Launch of Operation to Safeguard EU's Recovery Fund

On 15 October 2021, the EU and 19 Member States launched a new framework operation code-named "Sentinel" at the headquarters of Europol in The Hague. The operation will target frauds and other criminal activities against the EU's post-pandemic support under the Recovery and Resilience Facility (RRF). It will focus on proactive intelligence sharing, information exchange and supporting the coordination of operations for at least one year. Next to Europol, the EPPO, OLAF and Eurojust will support the operation. The RRF is the key initiative of the European Commission amounting to €672.5 billion in loans and grants to fight the economic and social impact of the Covid-19 crisis, to support EU citizens and businesses (→eucrim 3/2020, 174). (TW)

EP: Revision of Financial Regulation Needed

In a resolution of 24 November 2021, the European Parliament calls for a revision of the EU's 2018 Financial Regulation applicable to the general budget of the Union. Following the entry into force of the multiannual financial framework (MFF) 2021–2027 and against the background of the new form of EU spending via NextGenerationEU (NGEU), the EP considers the need for an update of the general rules for the EU budget. In addition, the revision should take into account innovations within the budgetary system and ensure the proper implementation of the EU budget. The Financial Regulation should be made subject to targeted improvements and simplifications, in particular where transparency, accountability and democratic scrutiny can be

increased. New financial rules should pursue the following objectives:

- Reinforcing the protection of the Union's financial interests;
- Ensuring alignment with the rule-of-law conditionality;
- Strengthening public procurement rules to avoid any potential conflict of interests;
- Increasing transparency;
- Reducing the administrative burden for beneficiaries;
- Strengthening the efficacy of spending with a view to achieving greater European added value;
- Increasing access to EU funding for citizens, SMEs and local and regional authorities.

The resolution makes detailed recommendations on these issues. It also sees the need to improve current audit, control and discharge procedures. Among other things, the European Public Prosecutor's Office (EPPO) should be included in the Financial Regulation. (TW)

EP Resolution: Digitalisation of the European Reporting, Monitoring and Audit

On 23 November 2021, the European Parliament (EP) adopted a resolution on the digitalisation of the European reporting, monitoring and audit. The EP points out that currently a bulk of reporting systems exist regarding the funds for the Common Agricultural Policy (CAP) as well as the structural and cohesion policies. This fragmentation of data makes the identification of final beneficiaries extremely difficult, if not impossible, for direct, indirect or shared management Union funds. In general, the current system is detrimental not only to the transparency of EU spending, but also to the oversight of the Union funds.

In order to enhance the protection of the Union budget and the European Union Recovery Instrument against fraud and irregularities, the EP suggests introducing standardised measures to collect, compare and aggregate information and figures on the final recipients and beneficiaries of Union funding, for the purposes of control and audit. To ensure effective controls and audits, it is considered necessary to collect data on those ultimately benefitting, directly or indirectly, from Union funding under shared management and from projects and reforms supported under the Recovery and Resilience Facility, including data on beneficial owners of the recipients of the funding.

The Commission should make available an integrated and interoperable information and monitoring system. This digital system should include the following features:

- A single data-mining and risk-scoring tool;
- Possibility to access, store, aggregate and analyse the aforementioned data on beneficiaries;
- Mandatory application of the system by the Member States;
- Capability for efficient checks on conflicts of interests, irregularities, issues of double funding, and any misuse of the funds;
- Access to the system by OLAF and other Union investigative and control bodies in order to exercise their supervisory and control functions.

The resolution calls on the Commission to initiate the appropriate legislative steps and to develop the proposed digital system. (TW)

ECA Report on Regularity of Spending in EU Cohesion Policy

On 23 November 2021, the European Court of Auditors (ECA) published a report on the European Commission's estimate of error in EU cohesion policy. The ECA pointed out that the related error rates, as disclosed by the Commission, are likely to underestimate the real level of irregularity in cohesion policy spending because of shortcomings in the Commission's control system.

The EU's cohesion policy aims to reduce development disparities between the EU Member States and regions. However, it is an area in which the risk of irregular spending is high, because the governing rules are complex and much of the expenditure is based on the reimbursement of declared costs.

In order verify the Member State auditors' work and findings, the European Commission carries out own verifications and assessments after Member State audit authorities have completed their audits of cohesion expenditure. With these findings, the Commission aims to confirm whether the residual level of error in cohesion spending reported by Member States is below the 2% threshold.

With regard to the 2014–2020 period, the ECA noted that the European Commission released the 10% payment retention initially withheld even if it had evidence that the expenditure in the accounts contained a level of error above 2%. This release is not in line with the overall objective of the payment retention, which was designed to safeguard the EU budget.

The ECA criticised the limitations of desk reviews by the Commission that are used to check the consistency of the regularity information that the Member States provide; this leads to undetected and uncorrected irregular expenditure. With regard to compliance audits, where the Commission reviews the eligibility of operations and related expenditure, the ECA pointed out the high frequency of undetected errors by the Commission. Therefore, the EU auditors concluded that the Commission likely underestimates the real level of error in cohesion policy in its annual management and performance report. (AP)

ECA Special Report on Performance-Based Financing in Cohesion Policy

On 21 October 2021, the European Court of Auditors (ECA) published its Special Report 24/2021: Performance-based financing in Cohesion policy. The 2014–2020 common provisions regulation introduced three instruments giving Member States financial incentives to strive for results and optimise their use of funding:

- The requirement to fulfil specific prerequisites ('*ex-ante* conditionalities') to create an investment-friendly environment;
- A mandatory performance reserve of around €20 billion (6% of cohesion spending) to be allocated to successful programme priorities in 2019;
- Performance-based funding models, which linked EU financial support directly to pre-defined output or results.

In its audit, the ECA assessed the use of these instruments from 2014 to 2020 and examined in particular whether they were well designed to incentivise performance and shift the focus towards achieving results, whether the Commission and Member States used them effectively, and whether their use made a difference in the way Cohesion funding was allocated and disbursed. The audit showed that the Commission and Member States have been only partially successful in using the three instruments to make the financing of Cohesion policy more performance based. The ECA noted that the *ex-ante* conditionalities instrument has been more successfully used than the other instruments. It pointed out that Member States showed very limited interest in using the two new performance-based funding models (the 'joint action plans' and 'financing not linked to costs'). Regarding the mandatory performance reserve, the ECA noted that, in 2019, the Commission released 82% of the €20 billion performance reserve for the 2014–2020 period. Overall, the allocation of the performance reserve had only a limited impact on programme budgets. The ECA also found out that the introduction of the performance framework in the 2014–2020 period contributed to a cultural change in the financial management of Cohesion policy. However, performance-based financing is not yet a reality in Cohesion policy, and the three instruments did not make a noticeable difference to the way EU funding was allocated and disbursed.

The ECA further made the following recommendations to the Commission:
- Make best use of enabling conditions in the 2021–2027 period;
- Prepare the ground early for an effective mid-term review for the 2021–2027 period;
- Clarify the rules underlying the 'financing not linked to costs' funding model;
- Clarify the approach of providing assurance on EU funding through the "financing not linked to costs" model. (AP)

ECA Report on Results of EU Spending Programmes

On 15 October 2021, the European Court of Auditors (ECA) published its Report on the performance of the EU budget – Status at the end of 2020. In the report, the ECA examined the results achieved by EU spending programmes financed by the EU budget, based on performance information from the Commission and other sources, including its own recent audit and review work.

The report noted that, while some of the spending programmes were affected by the COVID-19 pandemic in 2020 (such as Erasmus+ activities, progress has been made – as indicated by the available information. The ECA stressed that the Commission had generally taken into account the lessons learned from the relevant evaluations and audits.

In the area of *Competitiveness for growth and jobs* the principal programmes are Horizon 2020 (H2020) for research and innovation and Erasmus+ for education, training, youth, and sport. The ECA remarked that Erasmus+ is valued by stakeholders and the public as a useful programme that achieves its objectives. Overall, the auditors noted the positive added value of the programme. Individuals participating in it report positive effects on their professional skills. Although the programme had a concrete effect on organisations, as it allows them to strengthen and broaden international networks, there is less evidence of fundamental changes to institutional or pedagogical practices. The COVID-19 pandemic had major disruptive effects in Europe and negatively impacted many Erasmus+ activities, especially individual activities requiring mobility.

In the area of *Economic, social and territorial cohesion* the auditors selected the European Social Fund (ESF) – which promotes employment and social inclusion, integrating disadvantaged people into society, and ensuring fairer life opportunities – for the performance analysis. The ECA found that the performance framework increased the availability of such information; however, the focus was on financial input and output rather than on results. The auditors noted that progress towards the Europe 2020 target on employment was positive but that, results were lacking, mainly due to the pandemic.

In the area of *Natural resources* – covering expenditure linked to policies on the sustainable use of natural resources and financing the Common Agricultural Policy, the Common Fisheries Policy (CFP), and environmental and climate action – the ECA selected the European Maritime and Fisheries Fund (EMFF) for its analysis. The EMFF supports the objectives of the Common Fisheries Policy – objectives such as addressing unsustainable fishing and preventing the degradation of the marine environment. The auditors commented that performance information produced or obtained by the Commission should reflect the results achieved through the EMFF intervention, highlight any unsatisfactory progress, and trigger corrective action. The ECA stressed that the CFP target of reaching the desired conservation status for all fish stocks by 2020 is unlikely to have been met and criticises the key indicator used to monitor progress in this area (fishing at maximum sustainable yield levels), as it does not contain sufficient information indicating the level of progress made. The auditors pointed out that problems persist in regard to the fisheries control system,

which is a crucial factor in implementing the objectives of the CFP.

In the area of *Security and Citizenship* the ECA decided to analyse the Internal Security Fund Borders and Visa (ISF-BV), an instrument that provides support for border measures. The auditors noted that the ISF-BV has provided substantial support to help Member States handle the costs and challenges that emerged during the migration crisis and which have put enormous pressure on the EU's external borders. They concluded that the indicator measuring progress in accomplishing the instrument's overarching objective had been too broadly defined, undermining conclusions on the fund's overall performance. Regarding the specific objective of support for a common visa policy, the report pointed out that the ISF-BV has helped upgrade more than 2,620 consulates, thereby creating more secure and efficient visa processing centres.

Regarding the area of *Global Europe* the ECA analysed the performance of the Instrument for Pre-accession Assistance II (IPA II), which provides pre-accession assistance to candidate countries and potential candidates. The auditors observed that the indicators reported by the Commission in the programme statement show a modest performance for IPA II. While IPA II contributed to modernisation in the agri-food and rural development sectors, the auditors concluded that the overall progress of IPA II beneficiaries' economic, social, and territorial development is slower than expected. (AP)

Money Laundering

7th European Money Mule Action Concluded

On 1 December 2021, Europol published its conclusions on the seventh European Money Mule Action, Operation EMMA 7. This international action was coordinated by Europol and involved 27 countries, Eurojust, INTERPOL, the European Banking Federation (EBF), and the FinTech FinCrime Exchange. Around 400 banks and financial institutions supported the action. It targeted the laundering of criminal profits through money mule networks and represented a concerted effort against money laundering in Europe, Asia, North America, Columbia, and Australia.

EMMA provided a way for all these actors to cooperate and share intelligence, with the aim of identifying possible money mules. As a result, 7,000 fraudulent transactions were reported, 18,351 money mules and 324 recruiters/herders identified, 1803 individuals arrested, and a total loss estimated at nearly €70 million prevented. Money mules are persons who, often unwittingly, transfer illegally obtained money between different accounts on behalf of others. They are regularly tricked by criminal organisations that promise easy money. (CR)

Tax Evasion

Pandora Papers: EP Calling for Investigations and Improvement of EU Blacklist of Tax Havens

On 21 October 2021, the European Parliament adopted a resolution calling for thorough investigations to be launched into any wrongdoing that took place in EU jurisdictions as revealed by the Pandora Papers. After the Pandora Papers had exposed tax avoidance on an unprecedented scale, MEPs wanted to close loopholes currently allowing tax avoidance, money laundering, and tax evasion.

The MEPs stressed the importance of implementing already existing rules and are calling for better cooperation among national authorities across the EU. They criticised that numerous Member States are behind in the implementation of existing rules intended to counteract money laundering and tax avoidance, calling for legal action to be taken by the Commission against these EU countries.

The MEPs asked the Commission to analyse whether further legislation needs to be proposed and to establish whether legal action against some Member States is warranted. The MEPs also asked the European Public Prosecutor to assess whether the revelations merit any specific investigations.

In regard to the Pandora Papers, the MEPs label the current EU blacklist of tax havens a "blunt instrument," which is unable to catch some of the worst-offending countries. They put forward the fact that the British Virgin Islands account for two thirds of the shell companies in the Pandora Papers and yet they did not feature on the EU blacklist. The MEPs therefore propose improving the listing process (e.g. widening the scope of practices considered typical markers of a tax haven and reforming the process of deciding which jurisdictions are to be included). (AP)

Cybercrime

New Draft Law: EP Aims at Strengthening EU-Wide Requirements for Cybersecurity Attacks

On 22 November 2021, the European Parliament (EP) backed a draft law that would set tighter cybersecurity obligations in terms of risk management, reporting obligations, and information sharing for businesses, administrations, and states. The EP sees a need for this law because of the increase in cybersecurity attacks throughout 2020 and 2021. The EP can now start trilogue negotiations with the Council and the Commission on the planned new legislation. The Commission tabled the proposal for a Directive "on measures for a high common level of cybersecurity across the Union" in December 2020 (→eucrim 4/2020, 282–283). It will repeal Directive 2016/1148 on security of network and information systems (NIS Directive).

The new Directive will include an incident response, supply chain security,

encryption, and vulnerability disclosure. Member States will be able to identify smaller entities with a high security risk profile, and the highest managerial level would become responsible for cybersecurity.

The new directive will oblige more entities and sectors to take measures covering "essential sectors" (e.g. energy, transport, banking, public health, digital infrastructure and public administration). In addition, the new rules will also protect so-called "important sectors" (e.g. postal services, waste management, digital service providers, and the manufacturing of chemicals, food, medical devices, electronics, machinery, and motor vehicles). All medium-sized and large companies in selected sectors will also be covered by the legislation. The directive aims at establishing a European vulnerability database and a framework for better cooperation and information sharing between various authorities and EU Member States. (AP)

Several Hits Thwart Cyber Attacks

In a series of operations throughout October and November 2021, Eurojust helped facilitate the arrests of numerous online scammers, suspects involved in buying or selling illicit goods on the Dark Web, and attackers using ransomware. By supporting operation Dark HunTOR, Eurojust contributed to the arrests of 150 alleged suspects across Europe and the United States involved in buying or selling illicit goods on the Dark Web. Additionally, more than EUR 26.7 million in cash and virtual currencies were seized as well as 234 kg of drugs and 45 firearms. The operation built on the results of the takedown of DarkMarket, the world's largest illegal marketplace on the Dark Web, in January 2021.

Furthermore, through a series of actions, German, Georgian, and Israeli authorities dismantled a criminal network operating various online trading platforms and defrauding victims of millions of euros. Fraudsters had set up several limited companies, which operated these platforms and pretended to generate high profits on investments in financial securities, shares, commodity assets, currencies, and cryptocurrencies.

Twelve cyber actors involved in committing ransomware attacks against critical infrastructure focusing especially on large corporations were targeted in an action day carried out in the Ukraine and Switzerland. It included law enforcement and judicial authorities from eight countries as well as Europol and Eurojust.

A similar action against an organised crime group (OCG), which contributed to a considerable number of ransomware attacks across Europe, led to the arrest of two suspects and the seizure of multiple items. The estimated profits of the OCG amounted to several million euros and stemmed from their use of malware to render the data of companies and institutions inaccessible unless a ransom was paid. (CR)

Environmental Crime

Commission Proposal for Better Protection of the Environment by Means of Criminal Law

spot light

On 15 December 2021, the Commission adopted a proposal for a new EU directive to crack down on environmental crime. In this way, the Commission intends to fulfil a key commitment of the European Green Deal.

The proposal aims to make protection of the environment more effective by obliging Member States to take criminal law measures against environmental crimes. These crimes lead to increasing levels of pollution, a degradation of wildlife, a reduction in biodiversity, and the disturbance of ecological balance. They tend to be highly lucrative and can be as profitable as illegal drug trafficking. For this reason, environmental crimes are highly attractive for organised crime groups, *inter alia*, because sanctions are relatively low and because environmental crimes are prosecuted less often than other crimes. The main features of the proposal are as follows:

- Setting up new EU environmental criminal offences (including illegal timber trade, illegal ship recycling, and illegal abstraction of water);
- Clarifying existing definitions of environmental criminal offences in order to improve the effectiveness of investigations and prosecutions;
- Setting a common minimum denominator for sanctions on environmental crimes;
- Making relevant investigations and criminal proceedings more effective by implementing targeted and regular training (at all levels of the enforcement chain), overarching national environmental crime strategies, and awareness-raising measures;
- Improving cross-border cooperation by harmonising effective investigative tools and establishing an obligation to cooperate through Europol, Eurojust, and OLAF.

It is proposed to replace Directive 2008/99/EC, that got evaluated in 2020 by the Commission. The evaluation concluded that the Directive has had not enough effects on the ground because the number of environmental crime cases successfully investigated and sentenced remained very low. The proposal will now be negotiated by the European Parliament and the Council. (AP)

Commission Initiative to Achieve the European Green Deal

On 17 November 2021, the Commission adopted three new initiatives in order to achieve the European Green Deal. With these initiatives, the Commission aims to curb EU-driven deforestation, facilitate intra-EU waste shipments, promote a circular economy, and tackle the export of illegal waste and waste challenges to third countries. The three initiatives are the following:

- Proposal for a regulation on deforestation-free products: With these new rules, the Commission would like to guarantee

that the products that EU citizens buy, use, and consume on the EU market do not contribute to global deforestation and forest degradation. For its part, the Commission aims to reduce EU-driven greenhouse gas emissions and biodiversity loss. The objective of minimising the EU's contribution to deforestation and forest degradation will be achieved by establishing a tiered, mandatory due diligence system, relying on a definition of "deforestation-free," combined with a benchmarking system. The proposal also requires products to have been produced in compliance with the deforestation-free definition and with the laws of the manufacturing country.

- Proposal for a new regulation on waste shipments: With this regulation, the Commission aims to protect the environment and human health against the adverse impacts that may result from the shipment of waste. Therefore, the provisions should facilitate the environmentally sound management of waste and reduce the overall impact of using resources, especially by improving resource use efficiency. The proposed measures are crucial for the transition to a circular economy.
- EU soil strategy for 2030: The Strategy sets a framework of concrete measures for the protection, restoration, and sustainable use of soils and proposes a set of voluntary and legally binding measures. By 2050, all EU soil ecosystems should be in a healthy condition and thus more resilient, which will require very decisive changes in this decade. Therefore, the Strategy proposes legally binding objectives in the context of the Nature Restoration Law, to limit drainage of wetlands and organic soils and to restore managed and drained peatlands. The Commission will assess the need for and potential of legally binding provisions for a "passport for excavated soil", in order to reflect the quantity and quality of the excavated soil and ensure that it is transported, treated, and reused safely elsewhere. The Commission urges Member States to set by 2023 their own ambitious national, regional, and local targets in order to reduce net land take by 2030. To promote sustainable soil management, the Commission will prepare a set of "sustainable soil management" practices. (AP)

Terrorism

Commission Assessed Added Value of Directive on Combating Terrorism

On 18 November 2021, the European Commission published a report that assessed the added value of Directive 2017/541 on combating terrorism. The Directive is the main criminal law instrument at the EU level to combat terrorism. It lays down minimum standards for the definition of terrorist offences and offences related to terrorism and for penalties, while at the same time granting rights to protection, assistance, and support to victims of terrorism. In September 2020, the Commission published a report that assessed the legislative transposition of the EU rules, which had to be done by 8 September 2018 (→eucrim 3/2020, 182). The present report goes beyond the mere assessment of transposition and includes a wider analysis of the relevance, effectiveness, efficiency, coherence, and EU added value, including the impact of the Directive on fundamental rights and freedoms (cf. Art. 29(2) of the Directive). Findings are based on desk research and field research, involving a number of EU and Member States' authorities as well as civil society organisations.

The Commission report lists several issues that contributed to the positive functioning of the Directive, e.g.:

- The objectives were generally achieved;
- Several improvements were triggered by the Directive, such as enhanced legal clarity and enhanced cooperation;
- Clear added value with regard to combating terrorism;
- Even though the Directive has had an impact on fundamental rights and freedoms, the limitations largely meet the requirements of necessity and proportionality;
- The Directive has not had a problematic impact on the rule of law.

Despite these positive issues, the report also found several shortcomings, which need to be addressed by the EU institutions and the Member States. Such issues include:

- Difficulties in proving terrorist intent, which mainly result from factual circumstances, e.g. if evidence is located abroad;
- Some Member States find it challenging to classify violent activities of right-wing extremism as acts of terrorism;
- Several challenges remain in relation to the assistance and protection of victims of terrorism: problems result, for example, from the fact that not all Member States have designated single contact points and the lack of a secure tool for exchanging information on individual situations.

The Commission concluded, *inter alia*, that more needs to be done to improve the use of battlefield information. It also stated that it will further monitor the implementation of the Directive and initiate infringement proceedings, if necessary. (TW)

Trafficking in Human Beings

JHA Agencies Publish Joint Report on THB

On 18 October 2021, the nine European Justice and Home Affairs Agencies (CEPOL, EASO, EIGE, EMCDDA, eu-LISA, Europol, FRA, Frontex, and Eurojust) – under the leadership of Eurojust – presented their first joint report on the identification and protection of victims of human trafficking. The report sets out the exact role of each of the nine agencies regarding the identification and protection of victims of human trafficking. It also lists the main activities undertaken by each agency to support the protection of such victims. (CR)

Racism and Xenophobia

Initiative to Extend List of EU Crimes to Hate Speech and Hate Crime

On 9 December 2021, the European Commission published an initiative to extend the list of EU crimes to hate speech and hate crime. The initiative follows a set of EU actions already in place to counter illegal hate speech and violent extremist ideologies and terrorism online, such as Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, the EU Code of Conduct on countering illegal hate speech online, the proposed Digital Services Act, the 2021 Regulation on addressing terrorist content online, and the EU Internet Forum.

The Commission reiterated that combating hate speech and hate crime is part of its actions to promote the EU's core values and ensure that the EU Charter of Fundamental Rights is upheld. Any form of discrimination, as laid down in Art. 19 TFEU, is prohibited. Hate crime and hate speech go against the fundamental European values set out in Art. 2 TEU. Freedom of expression, as one of the pillars of a democratic and pluralist society, however, must also be strongly protected. The Commission recognised that there has been a sharp increase in hate speech and hate crime in Europe during the past decade, especially through use of the Internet and social media.

The proposed extension of the list of areas of EU crimes to hate speech and hate crime is based on Art. 83(1) TFEU, which lays down an exhaustive list of areas of crime for which the European Parliament and the Council may establish minimum rules involving the definition of criminal offences and sanctions applicable in all EU Member States. Art. 83(1) TFEU further specified that based on developments in crime, the Council may adopt a decision identifying other areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.

The Commission justified the extension by pointing out that hate speech and hate crime were particularly serious crimes because of their harmful impacts on the individuals and on society at large, undermining the foundations of the EU. The Commission further argued that the cross-border dimension of hate speech and hate crime is evidenced by the nature and impact of these phenomena – a special need exists to address them on a mutual basis. It stressed that, according to the UN, there has been an alarming spike in online and offline hate speech and incitement in recent years that can be linked to changes in the social, economic, and technological environment. Factors contributing to this increase have been the COVID-19 pandemic and the Internet. For the Commission, only the identification of hate speech and hate crime as a new, distinct area of crime can enable an effective and comprehensive criminal law approach to these phenomena at the EU level. (AP)

Procedural Criminal Law

Procedural Safeguards

CJEU Rules on Mechanisms to Remedy Errors in the Indictment

On 21 October 2021, the CJEU ruled on the compatibility of the Bulgarian Criminal Procedure Code with Directive 2012/13 on the accused person's right to information (Case C-282/20).

➤ *Facts of the case and questions referred to*

In the case at issue, criminal proceedings were conducted against *ZX* for the possession of counterfeit money. During the trial proceedings it came to light that the prosecutor's indictment contained errors and omissions. However, according to the referring Specialised Criminal Court, Bulgaria, following a reform in 2017, the current Bulgarian Criminal Procedure Code does not provide for a mechanism to remedy such defects in the indictment after the pre-trial hearing (where, in the case at issue, all formalities of the indictment were approved), for example by referring the case back to the prosecutor.

Against this background, the referring court first asked about the compatibility of the Bulgarian legislation with Art. 6(3) of Directive 2012/13. According to Art. 6(3), Member States shall ensure that, at the latest on submission of the merits of the accusation to a court, detailed information is provided on the accusation, including the nature and legal classification of the criminal offence, as well as the nature of participation by the accused person.

Second, the referring court asked how it should proceed if the CJEU concluded that Union law precludes the Bulgarian rules in question.

➤ *Findings of the CJEU*

As to the first question, the CJEU referred to its previous case law that dealt with the compatibility of the Bulgarian criminal procedure code with the EU's procedural rights directives, in particular its judgment of 5 June 2018 in *Kolev and Others* (Case C-612/15 →eucrim 2/2018, 99). It follows from this case law that amendments to the charge must be disclosed to the accused person or his/her lawyer at a point in time when they still have the opportunity to respond effectively, before the stage of deliberation. In addition, it follows that the rights deriving from Art. 6(3) of Directive 2012/13 must be protected throughout the criminal proceedings and thus, in the present case, also after the pre-trial hearing in a criminal case. As a consequence, national legislation that does not allow to remedy procedural defects in the indictment after the pre-trial stage of the criminal proceedings must be considered incompatible with Art. 6 of the Directive.

As to the second question, the CJEU reiterated its case law that the national

court should first try to give national law an interpretation consistent with EU law. If the national court is unable to do so, it may disapply the national provisions in question. In the present case, the judges in Luxembourg pointed out that the referring court may interpret Article 287 of the Bulgarian Criminal Procedure Code in conformity with Art. 6(3) of Directive 2012/13 and Art. 47 CFR. Under certain circumstances, Article 287 allows the prosecutor to make amendments to the charges during a judicial investigation.

➤ *Put in focus*

Although the case seems to deal with peculiarities of the Bulgarian criminal procedure, the judgment is important in two respects: First, it summarises the CJEU's case law on the accused person's right to information during criminal proceedings. Second, the judgment stresses that Art. 6(3) of Directive 2012/13 has direct effect and any national court has, as an organ of a Member State, the obligation to disapply any provision of national law which is contrary to such a provision of EU law with direct effect. (TW)

Data Protection

AG: German, Irish and French Data Retention Rules Incompatible with EU Law

spot light

On 19 November 2021, Advocate General (AG) *Campos Sánchez-Bordona* tabled his opinion on pending cases before the CJEU that concern the question of whether national data retention regimes are compatible with EU law interpreted in light of the CJEU's previous case law on this matter. The basic question is whether national regimes that retain personal data generated in electronic communications for the access by law enforcement authorities transgress the limits set by Art. 15 of Directive 2002/58 (the "e-Privacy Directive"). This provision allows, to a limited extent, exceptions to the obligation to ensure confidentiality of electronic communications. The CJEU has established detailed case law on the possibility for national legislatures to retain data in this sense, above all in its judgements in *Tele2 Sverige/Watson* (Joined Cases C-203/15 and C-698/15 →eucrim 4/2016, 164), in *Ministero Fiscal* (Case C-207/16 →eucrim 3/2018, 155–157), and in the recent landmark judgments in *Privacy International/Quadrature du Net* (Cases C-623/17 and Joined Cases C-511/18, C-512/18 and C-520/18 →eucrim 3/2020, 184–186).

The pending cases refer to the data retention systems in Germany and Ireland. In addition, a French case dealt with the question whether the principles established in the previous case law are also valid if EU secondary law confers powers for the authorities to have access to traffic data. The AG stated, however, that all references for preliminary rulings deal with the retention of data in a general and indiscriminate manner, so that the answers can be inferred from the CJEU's previous case law, in particular in *Privacy International/Quadrature du Net*. In detail:

➤ *Joined Cases C-793/19 and C-794/19 (SpaceNet and Telekom Deutschland)*

This case concerns the compatibility of the German data retention regulations as designed in the Law on Telecommunications (Paragraphs 113a et seq. TKG). In the case at issue, the Federal Administrative Court (*Bundesverwaltungsgericht*) must decide on complaints lodged by two companies, which provide publicly available internet access services in Germany, against their obligations to retain traffic and location data under the TKG (→eucrim 3/2019, 176). The referring Federal Administrative Court stressed that the German legislature established several limits to data retention, including the requirement to store only certain telecommunications data of certain means of electronic communications and a significantly reduced storage period (4 weeks for location data, and 10 weeks for other data).

AG *Sánchez-Bordona* acknowledged the progress made in the German legislation showing the will to comply with the CJEU case law. However, the German rules constitute a general and indiscriminate data retention regime with storage obligations of a wide range of traffic and location data. The time limits did not remedy this situation and the storage of electronic communications must be more targeted. In conclusion, the AG found that the German data retention legislation cannot be upheld; it is still an unjustified serious interference with the rights to privacy and data protection (irrespective of the duration of storage).

➤ *Case C-140/20 (G.D. v The Commissioner of the Garda Síochána)*

In the Irish case, the importance of a general/universal data retention regime was demonstrated because the Irish police could identify a murder on the basis of metadata retained from discarded mobile phones. The referring Irish Supreme Court, before which the defendant challenged the validity of the Irish legislation to retain and make accessible telephony data, stressed that there are no less intrusive, equally effective means for the detection and prosecution of serious crimes.

Similarly to the German case, AG *Sánchez-Bordona* opined that only the protection of national security, which does not include the prosecution of offences (even serious ones), can justify a general and indiscriminate regime of traffic and location data retention. The Irish legislation has gone beyond the requirements of the e-Privacy Directive. In addition, the AG pointed out that the Irish legislation has not met the condition (as required by the CJEU case law) that access by the competent national authorities to retained data is subject to prior review by a court or an independent authority, because, under Irish law, the review is done internally by the *Gardaí* (the Irish police). Lastly, the AG reiterated with regard to the murder conviction that a national court cannot

limit in time the effects of a declaration of illegality of national data retention legislation incompatible with EU law.

➤ *Joined Cases C-339/20 and C-397/20 (VD and SR)*

The cases concern investigations against two suspects in France for having committed illicit insider dealings. The prosecution was mainly based on personal data relating to the use of telephone lines that were collected by the *Autorité des marchés financiers* (Financial Markets Authority). The referring *Cour de Cassation* asked whether there is an independent obligation for the national legislature to require electronic communications operators to retain connection data on a temporary but general basis in order to enable the administrative authority to comply with EU Directive 2003/6 and Regulation 596/2014. This secondary EU law on market abuse confers administrative authorities the power to "require existing telephone and existing data traffic records".

According to AG *Sánchez-Bordona*, the CJEU's case law in *La Quadrature du Net* is applicable to the case even though the EU Directive and Regulation on market abuse come into play. He argued that the processing of data traffic records set out in the EU legislation on market abuse must be interpreted in the light of the e-Privacy Directive, which constitutes the reference standard in this regard. Neither the EU Directive nor the Regulation on market abuse confer specific and autonomous powers to retain data. They merely authorise the access to these data. As in the other cases, the French system concerns data retentions for the fight against crime, but which is preventive, generalised and indiscriminate and thus lacks the balance to be made as underpinned by the CJEU in *La Quadrature du Net*. With regard to the criminal investigations against the two defendants, the AG again stressed that a national court cannot limit in time the effect of that incompatibility.

It remains to be seen whether the CJEU takes up the AG's views or whether the judges bench takes a more nuanced approach to the individual referrals. For a thorough analysis of the CJEU's case law on data retention and the demand for recalibrating EU legislation on this matter →article by A. Juszczak/E. Sason, published at the eucrim website on 8 September 2021. (TW)

Commission Adopted Adequacy Decision for South Korea

On 17 December 2021, the Commission finally adopted the adequacy decision for personal data transfers between the EU and the Republic of Korea, after having concluded talks and initiated the necessary steps in the first half of 2021 (→eucrim 2/2021, 99). As of 17 December 2021, 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.

In a joint press statement, *Didier Reynders*, Commissioner for Justice of the European Commission, and *Yoon Jong In*, Chairperson of the Personal Information Protection Commission of the Republic of Korea, highlighted the benefits from the adequacy decision for business and citizens. The adequacy decision, which is based on the EU's General Data Protection Regulation, covers both data transfers for commercial and regulatory purposes. The Republic of Korea also benefits from the adequacy decision since it acknowledges a high data protection level in the country and thus facilitates data transfers with other non-EU countries which recognise the EU's assessment, such as Argentina, Israel, and Switzerland.

The adequacy decision includes a detailed assessment of the Korean data protection law, i.e. the Personal Information Protection Act (PIPA). An annex includes information about the legal framework of the Republic of Korea regarding the collection and use of personal data by Korean public authorities for law enforcement and national security purposes. (TW)

Victim Protection

EP Increases Efforts to Counteract Strategic Lawsuits Against Public Participation (SLAPPs)

On 11 November 2021, the European Parliament adopted a resolution on strengthening democracy and media freedom and pluralism in the EU. This follows after several initiatives had called for a regulation of Strategic Lawsuits Against Public Participation (SLAPPs):

- The 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, which recommended that the EU take legislative initiative with regard to SLAPPs (→eucrim 2/2021, 102);
- The statement by 119 organisations issued on 8 June 2020 (→eucrim 2/2020, 106).

In their resolution, the MEPs proposed a series of measures to counteract the threat that SLAPPs pose to persons with a watchdog function (e.g. journalists, NGOs, and representatives from civil society) in Europe. SLAPPs are lawsuits or other legal actions, as well as the threats of such actions, brought forward by powerful actors (e.g. private individuals and entities, public officials, public bodies, and publicly controlled entities) using a variety of legal bases, mostly in civil and criminal law. The purpose of these actions is to prevent investigation and reporting on breaches of Union/national law, on corruption, or on other abusive practices or to block or otherwise undermine public participation.

The MEPs stressed that SLAPPs are often meritless and based on exaggerated and often abusive claims that are initiated to intimidate, professionally dis-

credit, harass, wear out, put psychological pressure on, or consume the financial resources of those they target, with the ultimate objective of blackmailing and forcing them into silence through the judicial procedure itself. They see this practice as having a direct and detrimental impact on democratic participation, societal resilience, and dialogue – silencing the diversity of critical public thought and opinion. SLAPPs constitute direct attacks on the exercise of fundamental rights and have effects on the rule of law, posing threats to media freedom and public democratic participation, including freedom of expression, freedom of information, freedom of assembly, and freedom of association. In particular, the MEPs expressed concern over the fact that SLAPPs are increasingly being funded directly or indirectly from state budgets and being combined with other indirect and direct state measures against independent media outlets, independent journalism, and a free civil society.

The MEPs pointed out that SLAPPs not only undermine the right of effective access to justice but also constitute a misuse of Member States' justice systems and legal frameworks (e.g. by hampering the ability of Member States to successfully address ongoing, common challenges as outlined in the Justice Scoreboard). They urged the Commission to propose measures to address SLAPP cases, such as rules for the early dismissal of SLAPPs and other court actions that have the purpose of preventing public participation, which should include appropriate sanctions such as civil penalties or administrative fines. The Commission should also raise awareness of SLAPPs among judges and prosecutors across the Union. (AP)

Freezing of Assets

CJEU: National Legislation Must Allow Third Parties to Appear as a Party in Confiscation Proceedings

In its judgement of 21 October 2021 (Joined Cases C845/19 and C863/19 – *Criminal proceedings against DR and TS*), the CJEU clarified specific provisions of Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union. The CJEU precludes national legislation which allows for confiscation, in favour of the State, of property allegedly belonging to a person other than the perpetrator of the criminal offence, without that person having the right to appear as a party in the confiscation proceedings.

➤ *Facts of the case*

Two Bulgarian citizens were sentenced to a term of imprisonment and a fine in Varna (Bulgaria) for possession of highly dangerous narcotics without authorisation and with the intent of distribution. During a search of their respective homes, conducted in the context of pre-trial proceedings, a sum of money had been discovered.

Following the criminal conviction, the *Okrazhna prokuratura* – Varna (Regional Public Prosecutor's Office, Varna) applied to the *Okrazhen sad Varna* (Regional Court, Varna) for confiscation of this sum of money, in accordance with the Bulgarian criminal code. Before the court, the defendants stated that these sums of money belonged to family members. In accordance with national law, the family members could take part in the proceedings before the court.

The *Okrazhen sad Varna* (Regional Court, Varna) refused to authorise the confiscation of the sums of money, taking the view that the criminal offence of which the persons concerned had been convicted (i.e. possessing narcotics for the purposes of their distribution) did not have the purpose of generating economic benefit and that the persons concerned had neither been charged with nor convicted of said criminal offence. The Public Prosecutor's Office brought an appeal against the judgment of the Okrazhen sad Varna (Regional Court, Varna) before the referring court, arguing that the first instance court had not applied Art. 53(2) of the Bulgarian Criminal Code in the light of Directive 2014/42.

➤ *Question referred*

In these circumstances, the *Apelativen sad* – Varna (Court of Appeal, Varna) decided to stay the proceedings and ask the Court of Justice whether Directive 2014/42 only applies in cross-border situations. It further referred questions concerning the extent of the confiscation provided for by this directive and the scope of the right to an effective remedy by a third party who claims, or in respect of whom it is claimed, that he or she is the owner of property that is subject to confiscation.

➤ *Findings of the Court*

The judges in Luxembourg found that the possession of narcotics for the purpose of their distribution lies within the scope of Directive 2014/42, even though all the elements inherent in the commission of this offence are confined to a single Member State. The Court also found that Directive 2014/42 provides for the confiscation of property belonging to the perpetrator in respect of which the national court hearing the case is satisfied that it derives from other criminal conduct. The CJEU pointed out that it is necessary that the proceeds whose confiscation are being contemplated arise from the criminal offence in respect of which the perpetrator is ultimately convicted.

With regard to extended confiscation, the CJEU establishes two steps to determine whether a criminal offence is liable to give rise to economic benefit:

- First, Member States may take into account the modus operandi, for example whether the offence was committed in the context of organised crime or with the intention of generating regular profits from criminal offences;
- Second, the national court must be satisfied on the basis of the circumstances of the case, including the specific facts and available evidence, that the property was derived from criminal conduct.

The CJEU further found that confis-

cation from a third party presupposes establishing that a suspected or accused person has transferred proceeds to a third party or that a third party has acquired such proceeds and that that third party was aware of the fact that the purpose of the transfer or acquisition was to avoid confiscation. The Directive further requires Member States to take the necessary measures to ensure that the persons affected by the measures, including third parties who claim or in respect of whom it is claimed that they are the owner of the property whose confiscation is being contemplated, have the right to an effective remedy and a fair trial in order to uphold their rights.

In cases of extended confiscation, the Directive 2014/42 includes the right to be heard for third parties who claim that they are the owner of the property concerned, or who claim that they have other property rights. Since the Bulgarian law does not afford such a right, it is contrary to EU law. (AP)

Cooperation

Customs Cooperation

Launch of New Customs Risk Management System

On 1 January 2022, the EU started the operation of the new Customs Risk Management System (CRMS2). The system facilitates real-time exchange of information about security risks between customs administration of the 27 EU Member States. Risks may include health risks due to fake medical products, intellectual property rights infringements, environment and product safety risks, etc.

Paolo Gentiloni, Commissioner for Economy, said that "(t)he launch of this new system will deliver immense benefits for European customs authorities. It will mean that when dangerous goods are stopped at one point on the EU's external border, this information will be instantly shared among customs offices throughout the Union." He also stressed that CRMS2 will save the EU's financial interests.

CRMS2 will connect 6,500 customs officers and risk experts, covering all parts of the EU external border. The CRMS is the key element in the EU's customs risk management framework (CRMF). (TW)

Police Cooperation

Commission Proposes EU Police Cooperation Code

spot light

On 8 December 2021, the European Commission published three legislative proposals introducing a "EU Police Cooperation Code." The initiative is designed to enhance law enforcement cooperation across Member States and to give EU police officers more modern tools for information exchange. The proposed police cooperation package includes the following proposals, which are described in detail below:

- Council Recommendation on operational police cooperation;
- Directive on information exchange between law enforcement authorities of Member States;
- Regulation on Automated Data Exchange for Police Cooperation (Prüm II).

The proposed Council Recommendation on operational police cooperation aims at addressing obstacles to operational cooperation when police officers operate in other Member States, especially with regard to cross-border hot pursuit, cross-border surveillance, and joint patrols/operations. Furthermore, it sets out measures to enhance cross-border operational police cooperation in order to counter migrant smuggling and cross-border crime linked to irregular migration as well as to counter trafficking in human beings and to identify and protect victims. Measures are proposed to expand the current tasks of Member States' Police and Customs Cooperation Centres and to set up a single coordination platform for joint operations. Member States are encouraged to ensure effective access to information and communication by officers from the competent national law enforcement authority involved in cross-border operational police cooperation. Lastly, the recommendation provides a number of measures to enhance joint training and professional development.

The proposal for a Directive on information exchange between law enforcement authorities of the Member States seeks to establish rules for the exchange of information for the purpose of preventing, detecting, and investigating criminal offences. Under the proposed Directive, information exchange would be based on Single Points of Contact established or designated by the Member States. Detailed provisions would regulate the establishment, tasks, capabilities, and composition of these Single Points of Contact as well as the receipt and refusal of information through them. Additional rules govern judicial authorisation, protection of personal data, provision of information to Europol, and the use of SIENA (Europol's Secure Information Exchange Network Application) The proposed Directive would repeal Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU – also known as the "Swedish initiative."

The third instrument in the package, the proposal for a Regulation on Automated Data Exchange for Police Cooperation (Prüm II), aims to improve, streamline, and facilitate the exchange of information with Europol and between Member States' law enforcement authorities for the purpose of the prevention, detection, and investigation of criminal and terrorist offences. The scope of the draft Regulation applies to national databases used for the auto-

mated transfer of DNA profiles, dactyloscopic data, facial images, police records, and certain vehicle registration data. The proposal sets out rules for the use of these data by looking at various issues, e.g. principles of exchange, automated searching, reference numbers, rules for requests and answers, keeping of logs, etc. It also sets out common provisions, such as the designation of National Contact Points. Furthermore, the proposed Regulation provides a technical architecture for the exchange of data by introducing the use of a router to facilitate the establishment of connections with Europol and between Member States to query, retrieve, and score biometric data. Several provisions detail the use of the router, the launching of queries, the keeping of logs, quality checks, notification procedures, etc. An important issue in this context concerns rules on interoperability for the purpose of law enforcement access between the router and the Common Identity Repository (CIR) – a shared container for identity data, travel document data, and biometric data of persons registered in the EU's information systems, i.e. the EES, VIS, ETIAS, Eurodac, and ECRIS-TCN. The draft Regulation also establishes the steps for the exchange of data following a match. Ultimately, it regulates access by Member States to third country-sourced biometric data stored by Europol as well as access by Europol to data stored in Member States' databases.

Other chapters of the draft Regulation provide provisions on data protection and on the responsibilities of the Member States, Europol, and eu-LISA during the design, development, and start of router operation. The proposed Regulation would amend the current legal framework on the "Prüm cooperation," i.e. Council Decisions 2008/615/JHA and 2008/616/JHA, the legal framework on eu-LISA, and interoperability as set out in Regulations (EU) 2018/1726, 2019/817, and 2019/818. (CR)

European Arrest Warrant

CJEU: Amnesty Does Not Preclude Issuance of EAW

A European arrest warrant (EAW) may be issued even if the underlying criminal proceedings have been resumed after an amnesty. On 16 December 2021, the CJEU took this decision in Case C-203/20 and followed the opinion of Advocate General *Kokott* of 17 June 2021 (→eucrim 2/2021, 104). The judgment replies to a request for a preliminary ruling from a Slovak court. In 1998, the head of the Slovakian government had issued an amnesty in relation to crimes committed by some Slovakian security officers, including the kidnapping of the son of the then Slovak President in 1995. As a result, the prosecution was discontinued, which had the effect of an acquittal under Slovak law. After the amnesty was revoked in 2017, all criminal proceedings were resumed.

The competent Slovak criminal court now intended to issue an EAW and therefore asked the CJEU in essence whether the *ne bis in idem* principle may preclude the issuance of such arrest warrant.

The CJEU took the view that the *ne bis in idem* principle had not been violated in the present case, since the proceedings had been discontinued without the Slovak courts having been able to rule on the criminal liability of the persons being prosecuted. The *ne bis in idem* principle can only be invoked if the criminal liability of the person concerned has been examined and a determination in that regard has been made. This was not the case with the amnesty in question. (TW)

CJEU: Surrender Provisions in TCA also Binding on Ireland

Do the provisions on the EAW and the surrender regime included in the Withdrawal Agreement (WA) and the Trade and Cooperation Agreement (TCA) between the UK and the EU fall under Protocol No. 21 and are thus not binding on Ireland, because the country had not opted in? Or had the EU a one-off competence to regulate all subject matters contained in the Agreements?

These questions were subject of the CJEU's ruling of 16 November 2021 in Case C-479/21 PPU (*SN and SD v Governor of Cloverhill Prison*). The case concerned the legal basis for the surrender of persons from Ireland to the UK. According to the referring Supreme Court of Ireland, the arrests may have been unlawful because the provisions on surrender in the WA and TCA fall within the Area of Freedom, Security and Justice (AFSJ) and which are therefore, in principle, not binding on Ireland under Protocol (No 21). According to this Protocol, Ireland is not bound by measures within the AFSJ unless it has expressed its wish to apply one of them (opt-in), but Ireland has not done so either when the UK withdrew from the European Union or when the TCA was concluded.

The judges in Luxembourg, sitting in for the Grand Chamber, had to examine the question whether Art. 50(2) TEU (which provides for the European Union's external competence to conclude a withdrawal agreement) as the legal bases for the WA and Art. 217 TFEU (which lays down the competence to establish an association agreement) as the legal basis for the TCA were themselves appropriate as a basis for the inclusion of those measures in those agreements. Or whether a separate legal basis relating to the AFSJ would have been required, which would trigger the Irish opt-in possibility under Protocol (No 21).

The CJEU found that both the provisions of the WA which provide for the continuation of the EAW regime in respect of the UK during the transition period and the provisions of the TCA which provide for the application of the surrender regime established by that agreement to EAWs issued before the end of the transition period in respect of persons not yet arrested before the end of that period (→eucrim 4/2020, 265–271) are binding on Ireland.

As regards Art. 50(2) TEU, the CJEU argued that the EU had the sole competence to conclude an agreement setting out all arrangements for the withdrawal of a Member State; otherwise, there would have been the risk of treating areas in the Treaties inconsistently which would have prejudiced the withdrawal taking place in an orderly manner. Therefore, Protocol (No 21) could not apply.

Similarly, the CJEU argued in relation to Art. 217 TFEU that the TCA aims to have in place a broad relationship between the EU and the UK. The CJEU refers to its case law on acts pursuing several objectives and concludes that since the surrender mechanism introduced by the TCA pursues that objective alone, it is not necessary to add another legal basis. Hence, Protocol (No 21) is not applicable in relation to the TCA as well. (TW)

CJEU Clarifies Right to be Heard in EAW Cases

In the Joined Cases C-428/21 PPU and C-429/21 PPU (*HM and TZ*), referred by the Rechtbank Amsterdam, the CJEU had to deal with the question in which Member State and according to which procedures a person already surrendered must be heard if the issuing authorities requests the executing authority's consent as an exception to the specialty rule. In the two cases before the Rechtbank Amsterdam, the issuing authorities requested consent for the additional prosecution of offences committed prior to the surrender of the defendants, in accordance with Art. 27(3)(g) and (4) and Art. 28(3) of the Framework Decision on the European Arrest Warrant (FD EAW). The questions are not explicitly answered in the FD EAW.

According to the CJEU's judgment of 26 October 2021, a balance should be struck between, on the one hand, the effectiveness of the EAW mechanism, which is primarily based on the principles of mutual recognition and mutual trust, and, on the other hand, respect for the surrendered person's fundamental rights. The CJEU concluded the following:

- Since the right to be heard is one of the essential defence rights and is here closely connected with a judicial decision leading to the deprivation of liberty, the person concerned must have the opportunity to exercise his/her right to be heard in relation to a request for additional consent;
- The right to be heard must be exercised in respect of the executing judicial authority competent to deal with the request for additional consent (as provided for the above-mentioned provisions in Art. 27 and 28 FD EAW);
- The hearing can take place in the issuing state, but it must be guaranteed that the person had the opportunity to make known his/her views effectively and before the adoption of the decision by the requested authority;
- The executing judicial authority must ensure that it has sufficient information, in particular on the position of the person concerned, to take its decision on the request for consent issued pursuant to Art. 27(4) or Art. 28(3) FD EAW in full knowledge of the facts and with full respect for the rights of defence. If necessary, it must ask the issuing judicial authority to provide additional information without delay (applying Art. 15 FD EAW in analogy). (TW)

AG: Unlawful Appointment of Polish Judges Does Not Justify Non-Execution of EAWs *per se*

The CJEU was again asked to clarify its case law as to when EAWs from Poland can be refused due to the controversial justice reforms in the country and recent national court practice.

➤ *Background of the case*

Following its reference for a preliminary ruling in Joined Cases C-354/20 PPU and C-412/20 PPU (→eucrim 4/2020, 290–291), the *Rechtbank Amsterdam* sought further clarification on which consequences should be drawn for the execution of European Arrest Warrants issued in the country, following the problematic appointment of Polish judges in the wake of judicial reforms in Poland. In Joined Cases C-562/21 PPU and C-563/21 PPU, the *Rechtbank Amsterdam* essentially asked which criteria must be applied to be able to conclude whether or not the refusal of the execution of EAWs from Poland are justified or not. The following critical points were among the considerations:

- The controversial appointment of judges, which has not been in line with Union law (cf. the CJEU's recent case law on Poland →eucrim 3/2021, 135–137 and 2/2021, 71–72 with further references);
- The lack of remedies to challenge the appointment of judges, which infringes the individual's fundamental rights (right to a tribunal previously established by law) and consequently.

➤ *Opinion of AG Rantos*

In his opinion of 16 December 2021, Advocate General (AG) *Athanasios Rantos* reiterated the principles of the CJEU's case law on possible refusals due to the lack of judicial independence in the issuing country (cf. judgment in Case C-216/18 PPU (*LM*) →eucrim 2/2018, 104–105). In particular, a refusal is only possible in "exceptional circumstances" and the judicial authority executing EAWs must strictly stick to the two-step test established by the CJEU in *LM*. According to the AG, in the present case, this means that an irregularity in the appointment of judges cannot justify *per se* a real risk for the person concerned, namely that his/her case will not be treated in an impartial manner. The executing authority must ascertain that a real risk of violation of the fundamental right of the requested person to an independent tribunal exists and give reasons why it is believed that such a situation is likely to adversely affect the requested person's own case. The following points must be considered:

- The relevant conditions relating to his/her personal situation;
- The nature of the offences in question;

■ The factual context underlying the EAW.

Therefore, the circumstances leading to a real risk (that the person will not be tried by a tribunal previously established by law after surrender and that an effective remedy to challenge the composition of the court is lacking) do not exempt the *Rechtbank Amsterdam* from assessing the concrete risk of violation of the right to a fair trial for that person. In particular, it is incumbent on the *Rechtbank Amsterdam* to ascertain whether the person sought, once surrendered, runs the risk of his or her right to a fair trial being affected by the executive interfering in the competent courts.

Lastly, the AG examined the consequences of the recent decision by the Polish Constitutional Tribunal of 7 October 2021, which called into question the primacy of Union law (→eucrim 3/2021, 137). The premise must be to avoid impunity and not undermine the principle of mutual recognition. The fact, however, that there is currently no realistic opportunity for the defendant to challenge the controversial appointment of Polish judges, together with said reasons posing a real risk not to be tried fairly, may allow the *Rechtbank Amsterdam* reach the conclusion to suspend the execution of the EAWs.

➤ *Put in focus*

On the one hand, the AG stresses that there is no alternative solution other than to strictly follow the CJEU's two-step approach if the executing authority is concerned about violations of the fundamental right to a fair trial in the country that issued an EAW. It will remain difficult for national courts and the defendant to provide evidence of a concrete endangerment of this fundamental rights infringement in trials if the appointment of judges or the composition of courts is blamed. On the other hand, there is a silver lining, since the AG does not fully exclude the possibility of suspending the execution of Polish EAWs if, under the current case law of the Polish Constitutional Tribunal, there is no genuine possibility to challenge court compositions that have been established contrary to Union law. (TW)

European Investigation Order

CJEU: Bulgaria (Currently) Precluded from Issuing EIOs Due to Lack of Legal Remedies

On 11 November 2021, the CJEU ruled on the consequences of the peculiar Bulgarian legislation which has not provided for a legal remedy against (coercive) investigative measures and the issuance of a European Investigation Order (EIO) during the first stages of criminal proceedings. According to the judges in Luxembourg, the current situation infringes the fundamental rights of the Charter and means that Bulgaria cannot issue EIOs as long as this situation is not remedied.

➤ *Background of the case*

The case at issue (C-852/19, *Ivan Gavanozov II*) is a follow-up of a first ruling by the CJEU which answered the question how the Bulgarian authorities should fill in the EIO form if legal remedies are not foreseen in the Bulgarian legal order (→eucrim 1/2019, 36–37). The referring court, the *Spetsializiran nakazatelen sad* (Specialised Criminal Court, Bulgaria), was not satisfied with this answer and submitted a new reference for preliminary ruling asking for the substantial consequences of the current legal situation in Bulgaria.

The case in the main proceedings concerns criminal investigations against *Ivan Gavanozov* for large-scale VAT fraud. The Bulgarian authorities wished to request searches and seizures and a witness hearing from Czechia on the basis of an EIO, although Bulgarian law lacks any legal remedy both against the issuance of the EIO and the lawfulness of searches and seizures/witness hearings. The referring court opposed to this idea and asked the CJEU:

■ Whether Union law precludes legislation of a Member State which has issued an EIO that does not provide for any legal remedy against the issuing of an EIO the purpose of which is the carrying out of searches and seizures as well as the hearing of a witness by videoconference;

■ Whether Union law precludes the issuing, by the competent authority of a Member State, of an EIO, the purpose of which is the carrying out of searches and seizures as well as the hearing of a witness by videoconference, where the legislation of that Member State does not provide any legal remedy against the issuing of such an EIO.

➤ *Ruling of the CJEU*

The judges in Luxembourg followed the Opinion of Advocate General *Bobek* in this case (→eucrim 2/2021, 104–105). They shared his opinion that Art. 14(1) and Art. 1(4) of Directive 2014/41 regarding the EIO read in light with Art. 47 of the Charter does not leave discretion to an EU Member State whether it provides for legal remedies against the issuance of an EIO and investigative measures during the investigative phase. They justified this conclusion by the concept of mutual recognition and mutual trust: since, as a rule, the executing authority is required to recognise an EIO transmitted in accordance with Directive 2014/41, without any further formality being required, and ensure its execution in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing Member State, that authority must be sure that the issuing State complies with the EU's fundamental rights. This includes the persons' right to contest the need and/or lawfulness of an EIO and to obtain appropriate redress if an investigative measure has been unlawfully ordered or carried out.

Since the lack of legal remedies against the investigative measures in question and the issuance of an EIO in the current Bulgarian legislation infringes Art. 47(1) of the Charter and also rebuts the presumption of mutual trust, Bulgaria is not able to issue EIOs anymore.

➤ *Put in focus*

The CJEU's judgment strengthens the position of the individuals' fundamental rights in the EU scheme of mutual legal assistance. It can also implicitly inferred that the executing authorities are obliged to refuse the execution of EIOs if fundamental rights are not upheld in the issuing EU Member State in accordance with Art. 11(1) (f) of the EIO Directive. Nonetheless, the judgment concerns the specific Bulgarian situation where no legal remedies are foreseen in the investigative phase and it relates only to measures that encroach into fundamental rights. The latter, however, should be the case for most EIO requests. As the CJEU clarified, an infringement into the EU's fundamental rights also occurs if videoconferences are sought with witnesses. Not entirely solved is the question what persons who are affected by an EIO can do if there is no court in the issuing State, which examines the issuance of an EIO and takes an opposing position (to the law enforcement authorities), or if the issuing authorities ignore any justified objections against fundamental rights infringements in their country. For an analysis of the ruling in *Gavanozov II*, see also the op-ed by *Vânia Costa Ramos* at EU Law Live. (TW)

Law Enforcement Cooperation

Organisations Tell E-Evidence Stories and Urge to Uphold High Level of Fundamental Rights Safeguards

Following their open letter of May 2021 (→eucrim 2/2021,105–106), several civil society organisations maintained their criticism of the planned Regulation on European Production and Preservation Orders in criminal matters ("e-evidence Regulation" →eucrim 1/2018, 35–36). They published a compendium of scenarios that showcase situations in which the e-evidence Regulation would lead to serious fundamental rights concerns. The scenarios include:

- The media freedom and journalistic sources;
- The medical confidentiality and health data;
- The freedom to protest in Member States with systemic rule-of-law issues;
- The right to a fair trial.

The chapters highlight the fundamental rights at stake, describe hypothetical problematic situations involving the cross-border access to personal data and explain the necessary safeguards advocated for to mitigate fundamental rights harms.

In the light of the scenarios, the organisations make several recommendations to the EU policymakers. The compendium is designed to contribute to the ongoing trilogue negotiations on the EU's possible e-evidence legislation (→eucrim 1/2021, 38 and eucrim 3/2021, 164). (TW)

Third Edition of Digital Evidence Situation Report

On 24 November 2021, Europol, Eurojust, and the European Judicial Network (EJN) published the third annual edition of the SIRIUS European Union Digital Evidence Situation Report. In three chapters, the report provides reflections of the EU's law enforcement and judicial authorities as well as online service providers (OSPs) on the use of electronic evidence in the year 2020.

According to the report, the year 2020 was marked by the COVID-19 pandemic, leading to an acceleration in the digitalization of everyday life and in turn to criminals quickly adapting their activities to the situation. This created further challenges for the gathering and provision of electronic evidence.

From the perspective of EU law enforcement, the main challenges identified by the report continue to be the long delays in mutual legal assistance (MLA) and the lack of standardisation in OSP policies. However, 2020 was also marked by a positive development: For the first time, the SIRIUS platform – a secure web platform for law enforcement professionals that allows them to share knowledge, best practices, and expertise in the field of Internet-facilitated crime investigations – became the highest ranked source of information for law enforcement agencies seeking assistance when preparing direct requests.

Looking at the challenges that judicial authorities are facing, the length of MLA procedures when engaging with non-EU OSPs appeared to be a major concern. Other key issues identified include the lengths of data retention periods and the absence of data retention policies. Ultimately, the main challenge faced by OSPs in 2020 largely concerned the increased volume of data requests submitted by EU authorities.

Hence, to improve effective access to cross-border electronic evidence, the report sets out several recommendations:

- Under voluntary cooperation, EU law enforcement authorities are asked to use standardised templates for data preservation and disclosure requests and, if not already in place, to create single points of contact for electronic evidence requests to OSPs;
- EU judicial authorities are encouraged to stimulate national capacity-building initiatives as regards the instruments and procedures available to request and obtain electronic data from other jurisdictions and to enhance the interconnection, know-how, and exchange of expertise among EU judicial practitioners in the field of electronic evidence;
- OSPs are asked to join the SIRIUS Programme for OSPs if they have not yet done so; to disseminate updates about policies and changes in procedures to EU authorities, also through SIRIUS; and to take into account the perspectives of law enforcement and judicial authorities when updating their policies. (CR)

JHA Agencies Annual Meeting

On 22 November 2021, the nine European Justice and Home Affairs Agencies (CEPOL, EASO, EIGE, EMCDDA, eu-LISA, Eurojust, Europol, FRA, and

Frontex) met to sum up the activities and significant achievements of their network in the past year. In 2021, the network – under the Presidency of Frontex – focused on two strategic EU priorities, namely contributing to the European Green Deal and to digitalisation.

To contribute to a safer and cleaner environment, the network conducted a series of events in 2021 to discuss, for instance:

- The impact of climate change on migration and organised crime;
- EU and international efforts in fighting environmental crime;
- Ideas on how to make their administrations carbon-neutral;
- Digital solutions to make the Agencies more effective.

In addition, the Agencies signed a Joint Statement on the EU Green Deal, reaffirming their commitment towards the implementation of the European Green Deal and future green priorities. The event was attended by representatives from the European Commission, the European Parliament, the European External Action Service, and the General Secretariat of the Council as well as representatives from the current Slovenian Council Presidency and the upcoming French Presidency. (CR)

Network of Contact Points with South Partner Countries Established

In order to further implement the EuroMed Justice (EMJ) programme (→news of 12 November 2021), EU Member States and South Partner Countries agreed to set up the EuroMed Network of contact points (EMJNet) at the end of October 2021 in order to facilitate cross-border and cross-regional judicial cooperation. In a next step, authorities in the respective South Partner Countries (Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Tunisia, and Palestine – the latter shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue) will formally appoint their contact points. (CR)

Council of Europe

Reported by Dr. András Csúri (AC)

Foundations

European Court of Human Rights

ECtHR: Launch of HUDOC Case-Law Database in Bulgarian

On 8 November 2021, the Court launched the Bulgarian interface of its case-law database HUDOC, developed in cooperation with Bulgarian authorities. With more than 820 texts in Bulgarian uploaded from various partners, the interface shall further increase the understanding of the Court's case law among legal professionals and the general public. It joins the existing English, French, Georgian, Russian, Spanish, Turkish, and Ukrainian versions of the HUDOC database, which already contains over 33,000 case-law translations in 31 languages other than English and French.

ECtHR: Election of new Vice President and Section President

On 15 November 2021, the Court elected Judge *Síofra O'Leary* (Ireland) as new Vice President and *Marko Bošnjak* (Slovenia) as new Section President. They took office in January 2022.

Before joining the ECtHR, Ms *O'Leary* was Head of Unit of the Research and Documentation Directorate at the CJEU. She has been a judge at the ECtHR since 2 July 2015.

Prior to his career at the ECtHR, Mr *Bošnjak* worked in different positions at the University of Ljubljana and was an advisor to the Constitutional Court of Slovenia. He has been a judge at the ECtHR since 30 May 2016.

Human Rights Issues

CEPEJ: Action Plan on the Digitalisation of Justice

On 8–9 December 2021, the European Commission for the Efficiency of Justice (CEPEJ) adopted an Action Plan on digitalisation for a better justice. The four-year plan aims to reconcile the efficiency of new technologies and respect for fundamental rights (in particular Art. 6 ECHR), in order to guide states and courts in a successful transition to the digitalisation of justice. The CEPEJ adopted the following orientation:

- Efficiency of justice: supporting digitalisation of the administration and management of courts/prosecution services, in particular by ensuring that the tools chosen by States and courts are the most appropriate and compatible with quality, efficient, accessible, and impartial justice.
- Transparency of justice: promoting digitalisation to improve knowledge on justice in general and on the duration of proceedings in particular. Users should be better informed about the procedures, the judicial authorities and the respective tasks of each member of the judiciary. Each court should have dashboards that allow the monitoring and management

of its case flow; as a result, possible backlogs can be identified and limited, reasonable deadlines met and workload of justice professionals better managed.

- Collaborative justice: establishing user-friendly, compatible, and efficient digital communication tools for interconnectivity between participants in judicial proceedings.
- Human justice: adequately supporting the judges, prosecutors, their teams, and all other justice professionals by adapting their essential tasks to the digital environment. Digitalisation should make justice more efficient, but not replace the judge, who must remain at the centre of the proceedings.
- People-centred justice: supporting justice professionals and users through training so that they can make full use of digital tools. Training legal professionals, including lawyers, in the process of digital transformation contributes to both the efficiency of justice and its independence. Users who wish to do so should be supported, in particular through training, but proficiency in these digital tools should not become a condition for access to justice.
- Informed justice: increasing the use of the results of the CEPEJ evaluation of justice systems and other instruments. The CEPEJ should provide more analysed information and respond to other requests for specific analyses whenever possible.
- Responsible and reactive CEPEJ: ensuring the visibility of CEPEJ's tools so that they are accessible to all and reflecting the expertise of those who developed them. The CEPEJ is at the service of professionals and users of the justice system and has the task of using all the expertise at its disposal to respond quickly, concretely and efficiently to their requests.

CCPE: Opinion on the Practical Independence of Prosecutors

spot light

On 25–26 November 2021, the Consultative Council of European Prosecutors (CCPE) adopted Opinion No. 16 (2021) regarding the implications of decisions of international courts and treaty bodies on the practical independence of prosecutors. The Opinion is designed to guide States' judicial and prosecutorial reforms regarding the legislative framework for organisational autonomy of the prosecution services, the process of appointment, evaluation and dismissal of prosecutors, their term of office, the non-interference into their work and other important aspects relating to their career.

It underlines that the independence and autonomy of prosecutors and prosecution services should be encouraged and guaranteed by law, at the highest possible level, in a manner similar to that of judges.

With regard to the independence of the judiciary in general and of prosecution services/prosecutors in particular, the Opinion, *inter alia*, takes stock of the relevant case law of international courts (the ECtHR, the CJEU and the Inter-American Court of Human Rights), and relevant decisions of the United Nations treaty bodies. The case law of the international courts includes elements that contribute to strengthening the institutional independence of the prosecution authorities as well as the functional independence of the individual prosecutors. The main features in this regard include the following:

- The right to an independent and impartial tribunal as a core value of the rule of law. This guarantees the respect for human rights and fundamental freedoms and is crucial for public confidence in the judicial system in a democratic society. As the independence and autonomy of prosecuting authorities is a sine qua non for the independence of the judiciary, the indications contained in the relevant international judgments/decisions on the independence of the judiciary may, to a certain extent, also apply to prosecution authorities;
- Criminal justice systems rooted in different legal cultures differ across Europe. However, independence of law enforcement authorities as a prerequisite for the rule of law and independence of the judiciary has emerged as a factor of convergence in recent years;
- The ECtHR case law underlined that both the courts and the investigating authorities must remain free from political pressure in a democratic society. Thus, it is in the public interest to maintain confidence in the independence and political neutrality of a state's law enforcement agencies;
- Those in charge of the investigation must have no hierarchical or institutional connection to those being investigated and must also have practical independence – conditions for an effective investigation;
- Legal systems of those Member States in which prosecutors of higher rank have authority over prosecutors of lower rank, must foresee adequate arrangements to ensure the efficiency and independence of the bodies responsible for criminal investigations;
- The CJEU held that a prosecutor can be considered the issuing judicial authority for a European arrest warrant under certain conditions, in particular because the decision is subject to judicial review;
- The Inter-American Court of Human Rights, in line with the jurisprudence of the ECtHR, stated that one of the principal purposes of the separation of public powers is to guarantee the independence of judges and this should also be applied to prosecutors based on the nature of the duties performed by them.

The Opinion notes that the legal framework for the organisational autonomy of prosecution authorities (procedures for appointing, evaluating and dismissing prosecutors, their tenure, non-interference in the work of prosecutors and other important aspects related to their careers) can benefit from these case law. It also highlights that the following key elements of independence of prosecutors and prosecution services were established in previous CCPE opinions:

- Prosecutors must be free from unlawful interference in the exercise of their functions and from political pressure or

undue influence of any kind, including when acting outside the criminal law field;

- Similar to the judiciary, a corresponding legal framework should be in place that regulates the status, independence, recruitment, tenure of office and career of prosecutors on the basis of transparent and objective criteria;
- Prosecutors should have a career until retirement, as appointments for limited periods with the possibility of re-appointment bear the risk of prosecutors making biased decisions depending on the priorities of the appointing authorities;
- The external and internal independence of prosecutors and prosecution services should be ensured by an independent body such as a Prosecutorial Council;
- External and internal instructions given to prosecutors and law enforcement authorities should be based on guidelines that contain specific guarantees, e.g. the legality and transparency of instructions;
- The status, remuneration and treatment of prosecutors, as well as the allocation of financial, human and other resources to prosecutors, should be regulated according to the importance of their mission and work and in a manner comparable to that of judges;
- Prosecutors and, where appropriate, members of their families and livelihood, must be protected when carrying out their functions.

The opinion also takes a look at the decisions of national courts that strengthen the practical independence of prosecutors. Despite legal diversity, the following topics are discussed across several jurisdictions:

- Constitutional status and independence of the public prosecutor's office, its position and independence as well as autonomy, admissibility and limits of hierarchy within the prosecution service;
- Appointment and dismissal of prosecutors and prosecutor-generals, the transfer of chief prosecutors;
- Instructions, interference into the activity of public prosecution and the relation to the executive and legislative power;
- Salaries of prosecutors;
- Reporting on the activities of the public prosecutor's offices by the prosecutor-general;
- The position of the prosecutors in criminal proceedings and outside the field of criminal law.

CCJE: Opinion on Evolution of Councils for the Judiciary

During its 22nd plenary meeting, held online from 3 to 5 November 2021 in Strasbourg, the Consultative Council of European Judges (CCJE) adopted Opinion No. 24 (2021) "on the evolution of the Councils for the Judiciary". These are key bodies of judicial self-governance, which are called upon to safeguard judicial independence and impartiality. While reaffirming the principles set out in Opinion No. 10 (2007) on the Council for the Judiciary at the service of society, the CCJE took into consideration that political developments at both the international and domestic levels have made it necessary to reaffirm and complement the guiding principles. In this way, further guidance can be provided to policy-makers, legislators, and judges on essential aspects covering their role in independent and impartial judicial systems.

The Opinion argues that constitutions and international standards calling for the introduction and proper regulation of councils for the judiciary are not sufficient to ensure an independent judiciary. In the long term, the judiciary and other actors from government, politics, the media, and civil society must work together to strengthen professionalism, transparency, and ethics within the judiciary.

A council for the judiciary must have effective legal remedies in order to preserve its autonomy and to challenge the legality of public acts affecting it or the judiciary. It must also have legal standing before national and international courts. Its legitimacy must rest on a legal basis, reinforced by the public trust that is earned through transparency and accountability. To ensure its independence, the council must have sufficient resources and be accountable for its actions and decisions. The members of the council for the judiciary must meet the highest ethical and professional standards and be held accountable for their actions by appropriate means. The work of any council for the judiciary should be transparent, and its decisions and procedures should be sound and accountable – subject to judicial review, where appropriate. While there is no exclusive model for a council for judiciary, it must include adequate consequences to protect the independence of the judiciary and individual judges from undue influence in their decision-making.

As far as the careers of judges are concerned, any relevant decisions should be taken in a transparent procedure, preferably based on objective criteria. Decisions must be reasoned and, where necessary, be subject to judicial review.

Council members should be selected by means of a transparent process, avoiding even the slightest impression of political influence. Ex-officio membership is possible to a limited extent but should not involve members or representatives of the legislature or the executive. The majority of members should be judges elected by their peers, guaranteeing the widest possible representation of courts and instances as well as gender and regional diversity. The CCJE also proposes including non-judicial members to ensure a diverse representation of society.

Members should be appointed for a fixed term. The secure tenure of each member of the council is a fundamental prerequisite for its independence. Members may only be removed from office in the event of proven serious misconduct, in a procedure that guarantees their right to a fair trial. The Opinion concludes by requiring that the council and its members be fully committed to taking and supporting all appropriate steps to combat corruption within the judiciary.

Council of Europe Treaty	State	Date of ratification (r), signature (s), accession (a)
Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 223)	Albania Armenia North Macedonia Germany Uruguay Italy	28 January 2022 (s) 25 January 2022 (r) 26 November 2021 (r) 5 October 2021 (r) 5 August 2021 (r) 8 July 2021 (r)
Protocol amending the Additional Protocol to the Convention on the Transfer of Sentenced Persons (ETS No. 222)	Montenegro United Kingdom Italy	14 December 2021 (r) 7 October 2021 (s) 15 June 2021 (r)
Council of Europe Convention on Offences relating to Cultural Property (ETS No. 221)	Hungary	2 December 2021 (r)
Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (ETS No. 217)	Netherlands Switzerland	2 June 2022 (a) 25 May 2021 (r)
Council of Europe Convention against Trafficking in Human Organs (ETS No. 216	Costa Rica	24 November 2021 (r)
Council of Europe Convention on the Manipulation of Sports Competitions (ETS No. 215)	Morocco	20 September 2021 (s)
Protocol No. 16 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 214)	Montenegro Azerbaijan North Macedonia	13 December 2021 (s) 18 November 2021 (s) 9 September 2021 (s)
Fourth Additional Protocol to the European Convention on Extradition (ETS No. 212)	Portugal France	28 July 2021 (r) 10 June 2021 (r)
Convention on the counterfeiting of medical products and similar crimes involving threats to public health (ETS No. 211)	North Macedonia Mali	9 September 2021 (s) 29 June 2021 (s)
Convention on preventing and combating violence against women and domestic violence (ETS No. 210)	Liechtenstein	17 June 2021 (r)
Third Additional Protocol to the European Convention on Extradition (ETS No. 209)	France	10 June 2021 (r)
Council of Europe Convention on the Prevention of Terrorism (ETS No. 196)	Belgium	7 January 2022 (r)
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)	Luxembourg	21 October 2021 (r)
Additional Protocol to the Convention on the Transfer of Sentenced Persons (ETS No. 167)	Italy	15 June 2021 (r)
Second Additional Protocol to the European Convention on Extradition (ETS No. 98)	France	10 June 2021 (r)

Latest Update: 30 January 2022 (by *Clara Arzberger)*

Specific Areas of Crime

Counterfeiting

Committee of Ministers Declaration on MEDICRIME Convention

On 16 November 2021, the CoE Committee of Ministers published a declaration on the CoE Convention on the Counterfeiting of Medical Products and Similar Crimes Involving Threats to Public Health (the MEDICRIME Convention →eucrim 2/2016, 84–85). The MEDICRIME Convention, signed in Moscow on 28 October 2011, is the only international criminal law instrument aimed at preventing and combating threats to public health, including those arising from the COVID-19 pandemic. It identifies activities endangering public health as criminal offences, protects victims' rights, and provides the basis for efficient national and international cooperation. Issues concerning intellectual property rights are outside the scope of the Convention.

The Committee of Ministers reaffirms the key role of the Convention in guaranteeing and promoting the protection of public health by combatting the counterfeiting of medical products and other similar crimes. It is also committed to ensuring that the Convention is given the political support and the tools and means required to reinforce its effectiveness.

The declaration stresses that challenges, such as the COVID-19 pandemic, further highlight the importance of a strong and effective Convention. It underscores the need for one single, guiding committee to monitor implementation and improve States' capacity to prevent and combat counterfeit medical products and facilitate the Convention's effective use. The Convention is open for accession by any country in the world and currently has 18 States Parties. Another 18 states are in the process of ratification, which confirms the strong potential effect of this CoE Convention worldwide.

Cooperation

Law Enforcement Cooperation

Second Additional Protocol to Cybercrime Convention

On 17 November 2021, the Committee of Ministers of the CoE adopted a Second Additional Protocol to the Cybercrime Convention on enhanced cooperation and disclosure of electronic evidence. The second additional protocol lays down *inter alia* the criteria for direct cooperation between state parties and private entities when obtaining domain registration information or subscribing to data. The protocol provides a legal basis for:

- Disclosure of domain name registration information;
- Direct cooperation with service providers for subscriber information;
- Expedited cooperation and disclosure in emergency situations;
- Additional tools for mutual assistance, such as videoconferencing and joint investigation teams.

The text should be open for signature in May 2022.

CEPEJ Launches European Cyberjustice Network

On 16 November 2021, the European Commission for the Efficiency of Justice (CEPEJ) held a virtual inaugural conference to officially launch the European Cyberjustice Network. The network provides a platform for the interdisciplinary exchange of good practices in the field of cyberjustice and artificial intelligence. It also addresses challenges involved in the implementation of IT and artificial intelligence solutions in judicial systems. It is composed, in particular, of policy makers, ICT experts, judges, court staff, lawyers, and scholars. A major aim is to support the initiation of new tools, actions, and cooperation projects.

The recently adopted CEPEJ Guidelines on videoconferencing in judicial proceedings were also introduced at the conference. They provide a set of key measures to ensure compliance with the right to a fair trial.

Articles

Articles / Aufsätze

Fil Rouge

This eucrim issue looks at very recent developments in several areas of European criminal and "criminstrative" law. Debates on these issues have been underway for some time, but there is often a lack of viable proposals for solutions. In the articles, the authors present their own views, develop fresh perspectives on problems and encourage the reading audience to further discuss with their solution proposals.

In the first contribution, European Commissioner for Justice, *Didier Reynders*, outlines the various Commission proposals of 1 December 2021 to enhance digitalisation of the EU justice system – an urgent need that arose not only during the pandemic but also resulted from the implementation the digital transition of the EU. Digitalisation within the EU is one of the top priorities of the current Commission cabinet. The new initiative aims at modernising the EU justice systems. It addresses various challenges of digitalisation, including the use of digital tools for the communication between citizens/businesses and judicial authorities, improved cross-border exchange of information in terrorism cases via Eurojust, and a new collaboration platform for Joint Investigation Teams.

It must, however, also be made clear that the use of digital solutions and data brings benefits for citizens, on the one hand, but also entail risks to their privacy rights, on the other. In the second article, *Adam Juszczak* and *Elisa Sason* analyse one of the most controversial topics in this regard, i.e. how the EU should handle the retention of electronic communication data for law enforcement purposes. Following several landmark judgments, working groups rack their brains how the requests by the judges at Kirchberg can be appropriately implemented in fundamental-rights-proved rules. After having analysed in detail previous CJEU case law, the authors conclude that the CJEU's jurisprudence does not put an end to the ongoing discussions on data retention and that a recalibrated solution is needed by way of a common legislative approach at the EU level. It will be exciting to see whether the CJEU develops new lines of argument in the pending cases on the data retention regimes in Germany and Ireland.

Another pertinent issue in European law concerns *ne bis in idem* protection, and contributing author *Pierpaolo Rossi-Maccanico* points out several difficulties in interpreting the elements of this guarantee in the third article. He comments on the Advocate General's opinion in the two pending cases *bpost* and *Nordzucker* – both of which deal with parallel competition proceedings. He thoroughly analyses the case law of the European courts (CJEU and ECtHR) on the decisive element of *idem factum* and elaborates on the nuanced differences in the interpretation of the courts in competition, judicial cooperation, and tax law matters. He advocates a more sophisticated solution as to the interpretation of the *idem* element, depending on the area of law in which the *ne bis in idem* principle applies.

Subsequently, two contributions deal with topics of judicial cooperation. *Florentiono-Gregorio Ruiz Yamuza* tackles in his article the question of how to organise compensation for unlawful/unjustified detention in European Arrest Warrant cases – a widely neglected topic in legal literature so far. He highlights the relationship between compensation and the fundamental rights of the detained person and therefore with the provisions of the European Convention on Human Rights and the EU Charter of Fundamental Rights, and he outlines the frequently occurring difficulties in establishing the elements of unjust or arbitrary detention, especially when it comes to the enforcement of an extradition request. *Ruiz Yamuza* makes several recommendations on how the EU should proceed in developing a uniform legal framework on this matter.

Lastly, *Lennard Breulich* reports on a Council of Europe conference at which participants discussed current problems involving mutual legal assistance and extradition in Europe as well as the perspectives for future international cooperation in criminal law.

Thomas Wahl, Managing Editor of eucrim

Digitalising Justice Systems to Bring Out the Best in Justice

Didier Reynders

> My priority is to make the justice sector a forerunner during Europe's Digital Decade. I would like to see all barriers to access to justice removed and hope to restore the confidence of citizens and businesses in the efficiency of justice systems.

When citizens think of justice, they might think of lawyers in wigs, law courts with neoclassical pillars, or Lady Justice. But, in practice, this image of justice has changed over time, as have the tools at our disposal to support the pursuit of justice.

I am happy to report that justice in the European Union is advancing towards digitalisation steadily and ambitiously – in line with the trends of our century. Indeed, my priority is to speed up this work and make the justice sector a forerunner during Europe's Digital Decade. I would like to see all barriers to access to justice removed and hope to restore the confidence of citizens and businesses in the efficiency of justice systems.

When the COVID-19 pandemic started, many EU citizens experienced delays and sometimes a full halt to their justice systems. It became apparent that there is still room for progress in making justice systems more resilient and efficient, especially by making the most of the digital transition. On 1 December 2021, I presented three proposals to further modernise our EU justice systems:

The first suggestion aims to make the administration of justice easier and cheaper for citizens and businesses. According to this new proposal, they would be able to use electronic means of communication to file claims and to communicate with authorities from the safety of their homes or offices. Exchanges between Member States will be possible through national portals, and, at the same time, the European Commission will provide an access point for the European e-Justice Portal. We are looking at establishing a modern and integrated solution that tackles existing practical barriers. Citizens will also be able to pay court fees electronically. Moreover, given the lessons learned from the pandemic, our proposal ensures that oral hearings could also take place by means of videoconferencing.

Digital tools are not only useful for accelerating procedures and cutting travel time; they are also fundamental in ensuring our safety from criminal threats. The 2016 Brussels bombings were a coordinated terrorist attack that severely hit Belgium. Many fellow European citizens also experienced the grief and fear that these attacks caused, which are still threatening our societies. We are introducing two proposals that will make the manner in which we approach terrorist threats and criminal investigations more resilient and fit for our digital age.

In this context, the second proposal on digital information in cross-border terrorism cases is directed at significantly modernising Eurojust's information system. In fact, it was the aftermath of the 2015 Bataclan concert hall attack in Paris that made authorities realise they need better cross-border collaboration to counteract cross-border terrorist investigations and prosecutions. This realisation resulted in the creation of Eurojust's European Judicial Counter-Terrorism Register. I am proud to say that it has revolutionised the work of law enforcement authorities across the

EU, allowing prosecutors to identify potential links in investigations against terrorist suspects in different EU countries and to coordinate the judicial response. The coordinated involvement of judicial authorities is also crucial from a rule-of-law point of view, as coordinated preventive measures – such as house searches and arrest warrants – need to be authorised and supervised by judicial authorities.

We now aim to take the Register to the next level. We propose modernising the system to identify many links automatically, hence requiring much less manual intervention. This will enable Eurojust to provide faster and better feedback to national authorities. We also propose setting up secure digital communication channels between national authorities and Eurojust. Lastly, this proposal should establish a clear legal basis for cooperation with prosecutors outside the EU.

The third proposal involves supporting the functioning of Joint Investigation Teams (JITs). These teams are set up for specific criminal investigations put together by the authorities of two or more States to carry out criminal investigations together. According to the proposal, a Joint Investigation Teams collaboration platform would be established. The platform will be a highly secure online collaboration tool aiming to facilitate the exchanges and cooperation within JITs throughout their duration. It will provide for easy electronic communication, the exchange of information and evidence (including large amounts of data), the traceability of evidence as well as the planning and coordination of JIT operations. The platform is designed to be confidential; therefore, it meets the highest levels of cybersecurity standards.

In previous discussions and meetings with justice professionals, it struck me how much investigative judicial authorities rely on each other to exchange information and evidence securely and swiftly. I witnessed that having digital tools in place is crucial, especially when time is of the essence. In addition, citizens and businesses are operating digitally more and more, and they expect to get a digital and fast response to their issues.

As part of the NextGenerationEU, the digitalisation of justice systems has become a horizontal objective for all the Member States. I am proud to report that we are delivering on our promises to forge a modern and digital justice system. Member States will also need to implement all manner of tools and IT infrastructures. Together, we are creating a truly efficient and resilient European area of freedom, security and justice.

Didier Reynders, European Commissioner for Justice

Recalibrating Data Retention in the EU

The Jurisprudence of the CJEU – Is this the End or the Beginning?

Adam Juszczak and Elisa Sason*

Data retention has been subject of extensive and fierce discussions amongst practitioners, policy makers, civil society and academia in the EU and its Member States for many years – often coined as a clash between liberty and security. Through its jurisprudence, the Court of Justice of the EU (CJEU) attempts to find a balance between the fundamental rights and freedoms at stake. This article provides a legal analysis of the jurisprudence of the CJEU on data retention, from the Decision in Digital Rights Ireland/Seitlinger to the most recent Decisions in the Cases *Privacy Int.*, *Quadrature du Net* and *H.K. v Prokuratuur*. It observes that while the CJEU has reconfirmed its previous jurisprudence on data retention, it widely opens the door to a variety of exceptions. The analysis covers the implications of the most recent jurisprudence of the CJEU from a legal and practical angle and seeks to establish whether, on the basis of its findings, it is indeed possible to apply these exceptions in practice. Given the link with data retention, the current state of play of the negotiations on the e-Privacy Regulation between the European Parliament, Council and Commission is briefly reflected. The article concludes that the latest jurisprudence of the CJEU does not put an end to the ongoing discussions on data retention but that there is a need for a recalibrated solution by way of a common legislative approach, at least on a set of definitions and basic notions at EU level. This could provide for the desired added value and the necessary legal certainty for all stakeholders involved, also given the increasing number of cross-border investigations and prosecutions in the EU and the fact that service providers are established all over Europe and the rest of the world.

I. Introduction

Over the past years, data retention has been the subject of extensive, controversial and at times fierce discussions amongst practitioners, policy makers, civil society and academia in the EU and its Member States. Essentially, it is about the retention by providers of electronic communication services and networks of traffic and location data for a certain period of time, in order to allow access by competent national authorities for the purpose of preventing, investigating, detecting, or prosecuting crimes and safeguarding national security.

Although it is generally about traffic and location data and not about the content of the communication conducted, the scope of such retention remains significant. The kind of retained data enables obtaining an enormous amount of information, such as locating the source of a communication and its destination; determining the date, time, duration and type of communication; identifying the communications equipment used; locating the terminal equipment and communications; saving the names and addresses of users, the telephone numbers of the caller and the person called, and the IP address for internet services.

Data retention covers all electronic communication systems and applies to all users of such systems, not only to persons suspected of having committed a crime. It applies to all users of electronic communication, without distinction or exception. Some repeat that it is indispensable that electronic communication operators and service providers retain certain data – besides that collected strictly for their business purposes – and disclose it, under certain conditions, to law enforcement, judicial and other competent authorities, in order to effectively prevent serious threats to security and combat serious crimes, including terrorism, organised crime or child pornography.[1] Others reiterate that such practice constitutes an invasive and unjustified encroachment on fundamental rights; they also put in question the purported benefits of the retention of data for the purpose of preventing threats and fighting crime as such.[2]

The matter of data retention raises myriads of legal and practical questions and touches upon fundamental rights in the European multi-level system, i.e. fundamental rights as enshrined in national constitutions (national level), and those enshrined in the EU Charter of Fundamental Rights and the European Convention on Human Rights (European level). At the EU level, the Court of Justice of the European Union (hereinafter "CJEU") as the guardian of the Charter of Fundamental Rights[3] (hereinafter "Charter"), checks whether national legislation on data retention complies with Union law, and in particular the Charter. At the same time national Supreme Courts or Constitutional Courts are competent to check compliance of national provisions against the guarantees enshrined in their national constitu-

tions, while the European Court of Human Rights (ECtHR) reviews interferences with the European Convention on Human Rights (ECHR). This mixed and multi-layered judicial environment does not make it easy to attain clarity and certainty in establishing the scope and limits of data retention in Europe. It is hence not surprising that several national Supreme and Constitutional Courts rendered judgements on data retention in the past years,[4] as well as the ECtHR,[5] and, lastly, the CJEU.

For all the focus on the judicial and security dimension of this topic, another aspect related thereto remained out of sight: Imposing an obligation on providers of electronic communication services and networks to retain data and provide access thereto to competent national authorities, might not only potentially pose a significant financial burden on the service providers, but also comprises a considerable impact on the way they conduct their business – a right that falls under the scope of Art. 16 of the Charter. Although the CJEU has reviewed the requests for preliminary ruling by referring to fundamental rights of the Charter, it has been entirely oblivious to a potential interference with said Art. 16 of the Charter.

Generally, although the protection of personal data is high on the political agenda in the EU, there has always been strong political will to find a viable solution allowing for an effective use of retained data for the purpose of combating crimes and maintaining security in the EU. The heads of state and government underlined at the meeting of the European Council in December 2020 that it is essential that national law enforcement and judicial authorities exercise their powers both online and offline to combat serious crime and – in the light of the case law of the CJEU – stressed the need to continue and advance work on retention of data in full respect of fundamental rights and freedoms[6]. At the March 2021 Justice and Home Affairs Council, Ministers, too, stressed the need for competent national authorities to have access to data previously retained for the purpose of preventing, investigating, detecting, and prosecuting serious crimes.[7]

This article provides a short background on data retention at the EU level (II.) before it outlines the most recent jurisprudence of the Court of Justice of the European Union (III.). It subsequently elaborates on the legal and practical consequences of that jurisprudence (IV.), sheds light on this matter in the context of the current negotiations on the e-Privacy Regulation between the European Parliament, Council and European Commission (V.), and concludes with a number of reflections on how and to which extent retention of personal data and access thereto could be reconciled with the requirements under EU law (VI.).

II. Quick Flash: From the Data Retention Directive to the Tele2/Watson Decision by the CJEU

At the EU level, common rules on a Union-wide data retention regime were introduced back in 2006 by Directive 2006/24/EC,[8] which obliged Member States to adopt measures to ensure that providers of electronic communication services and networks retain traffic and location data (excluding the content of the communication) for between six months and two years, in order to allow access by competent national authorities for the purpose of investigation, detection and prosecution of serious crimes.

1. Digital Rights *Ireland/Seitlinger* – the CJEU's decision on the invalidity of the Data Retention Directive

This first and somehow candid attempt to establish an EU-wide data retention regime was, to some surprise of many, declared invalid by the CJEU in 2014 in its landmark decision *Digital Rights Ireland and Seitlinger*.[9] Following legal challenges in Ireland and Austria, requests for a preliminary ruling were made by the Irish High Court and the Austrian Constitutional Court (*Verfassungsgerichtshof*), and the CJEU held that the retention of data, as envisaged in that Directive, violated Arts. 7 and 8 of the Charter. The CJEU established that the general and indiscriminate retention of data envisaged in the Directive constituted a particularly serious interference with fundamental rights, as it was not sufficiently circumscribed to ensure that the interference is limited to what was strictly necessary. However, the CJEU did not fail to stress that in its view the retention of data genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security and that, as such, it does not adversely affect the essence of the fundamental rights in question. Moreover, the CJEU stated that the Directive may be considered appropriate for attaining the objective pursued – in other words, that the retention of data and access thereto by national authorities was considered a suitable tool that indeed has an added value in combating serious crimes.[10]

Although this decision has been perceived as marking the end to data retention in the EU, the CJEU clearly did not dismiss data retention as such but the way the directive was constructed – the Union legislator failed the proportionality test. The CJEU meticulously enumerated the faulty parts of the Directive, i.e.:

- The lack of differentiation, limitation or exception when retaining all traffic data of all individuals;[11]
- The lack of any objective criteria as regards the access to the data by national authorities;[12]
- An overly rigid retention period, without any distinction as

regards the categories of data and the usefulness for the objective pursued;[13]
- The absence of sufficient safeguards against the risk of abuse of the retained data;[14]
- An overly relaxed attitude allowing that the data may be retained outside the EU, hence out of reach of the required control of compliance under EU law, as also required by Art. 8(3) of the Charter.[15]

What was the immediate consequence of this decision? The CJEU declared Directive 2006/24 invalid but it did not dismiss data retention as such, thus leaving room for national solutions, provided they comply with the standards of EU law. As the CJEU does not consider the validity of national legislation transposing that Directive, its decision could not not directly impact the domestic regimes on data retention across the EU. Although a number of national courts of last resort declared national legislation to be invalid on the basis of the *Digital Rights* decision[16] and some Member States made limited amendments, it remained unclear to which extent the findings and requirements of that decision would, in practice, impact the domestic regimes on data retention.

It required further action to bring this matter before the CJEU again and to give practical effect to the landmark judgement in *Digital Rights*. This happened just a day after the decision of the CJEU, when Swedish telecommunication company "Tele2" decided to no longer retain data and informed the Swedish authorities accordingly. Legal proceedings were instituted and, in the course thereof, the Swedish court (*Kammarrätten i Stockholm*) referred the question whether national law governing a general and indiscriminate retention of data, where the objective pursued is not limited to fighting serious crimes,[17] was compatible with Directive 2002/58/EU[18] (hereinafter "e-Privacy Directive") and the Charter. The Swedish request was joined by a UK court request, which demonstrated how innocuous the *Digital Rights* decision was perceived, when the referring court (*Court of Appeal of England & Wales (Civil Division)*) asked, whether the judgement of the CJEU in *Digital Rights* laid down mandatory requirements of EU law applicable to a Member State's domestic regime on access to data retained in accordance with national legislation.[19]

2. *Tele2/Watson* – the CJEU's blueprint to check invasive legislative measures on data retention and access against the e-Privacy Directive as read in light of the Charter

In its judgment of 21 December 2016, the CJEU ruled that EU law precluded national legislation that prescribed a general and indiscriminate retention of traffic and location data.[20] By building upon and reconfirming analogously the line taken in *Digital Rights,* the CJEU set out in detail its systematic approach in reviewing the compliance of national provisions with Art. 15(1) of the e-Privacy Directive in the light of Arts. 7, 8, 11 and 52(1) of the Charter. Thus, the decision *in Tele2/Watson* forms in essence the blueprint for reviewing invasive legislative measures on data retention and access thereto against the relevant Union law. Thereby, the CJEU followed a two-step approach: first, it reviews compliance of the provisions requiring the retention of data by the providers with the above-mentioned provisions, second, it reviews compliance of the provisions allowing for access to that justifiably retained data by competent national authorities with said provisions of Union law.

By highlighting the high level of protection of personal data and privacy guaranteed by the e-Privacy Directive, the CJEU stressed that the principle of confidentiality enshrined in the e-Privacy Directive prohibits, as a general rule, the storage of traffic and related communication data by any person without the consent of the user.[21] Save for the technical storage necessary for the conveyance of the communication, the only exception to this rule is permitted by Art. 15(1), which enables Member States to derogate from the principle of confidentiality under certain conditions laid out therein.[22] The CJEU concluded that Art. 15(1) is to be interpreted strictly, meaning that the exception this provision allows must remain an exception and not become the rule.[23]

More concretely, the CJEU outlined that, according to Art. 15(1), Member States may adopt legislative measures derogating from the principle of confidentiality where "it is a necessary, appropriate and proportionate measure within a democratic society" to safeguard the list of objectives, i.e. national (State) security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences, or unauthorised use of the communication system. The CJEU further clarified that this list of objectives is exhaustive, and Member States cannot go beyond.[24] Moreover, it follows from Art. 15(1) that any national measure derogating from the principle of confidentiality needs to be in accordance with the general principles of EU law. This opens the avenue to checking the national legislative measures against fundamental rights enshrined in the Charter. In the same way as in *Digital Rights*, the CJEU considered the examination of the compatibility with Arts. 7, 8 and 11[25] of the Charter as pertinent. In this context, the CJEU explained that, pursuant to Art. 52(1) of the Charter, any limitations on the exercise of the rights and freedoms recognised by the Charter must be provided for by law, respect the essence of those rights and be proportionate, i.e. they must be necessary and meet objectives of general interest recognised by the EU or the need to protect rights and freedoms of others.[26] These requirements are echoed in

Art. 15(1) of the e-Privacy Directive, which states that data should be retained "for a limited period" and be "justified" by reference to one of the objectives mentioned in the same Article. This methodological approach is applied by the CJEU to the rules governing the retention of data (below (1)) as well as, at later stage, to those governing access to the retained data (below (2)). This is the benchmark against which the national law in question will be measured.

(1) With regard to retention, the CJEU concluded that the data retained allows very precise conclusions to be drawn concerning the private lives of the persons.[27] According to the CJEU, the fact that the persons concerned are not informed of their data being retained, is likely to cause a feeling of constant surveillance.[28] It held that the interference with Arts. 7 and 8 of the Charter was particularly serious and that only the objective of fighting serious crime was capable of justifying such serious interference.[29] The CJEU continued that even if the retained data concerns traffic and location data and not the content of communication,[30] this would have an effect on the use of means of electronic communication, and consequently, on the exercise of the user of the freedom of expression, guaranteed by Art. 11 of the Charter.[31]

In conclusion, national legislation providing for a general and indiscriminate retention of data, and where there is neither any requirement that there be a relationship between the retained data and the threat to public security, nor any other restrictions or exceptions, e.g. with regard to the time period, geographical area or group of persons, exceeds the limits of what is strictly necessary.[32] Legislation requiring such retention would in fact turn the exception envisaged in Art. 15(1) into a rule.[33]

In the same way as in *Digital Rights*, the CJEU did not dismiss data retention *per se.* Moreover, it instantly presented a possible remedy to the established disproportionality of the legislative measures under scrutiny in the case at hand: The CJEU referred to the idea of a targeted retention of traffic and location data for the purpose of serious crime. In the CJEU's view, this approach – provided it fulfils a number of strict conditions – would be a permissive way of retaining data as a preventive measure to allow access by competent national authorities.[34] The mentioned conditions include e.g. clear and precise rules on the scope and application of the retention measure, and minimum safeguards for persons affected. The CJEU stressed that the measure must be limited to what is strictly necessary, in particular it must be based on objective evidence to identify persons, whose data is likely to reveal a link – at least an indirect one – with serious criminal offences, and to contribute to fighting serious crime or preventing a serious risk to public security. By way of an example, the CJEU mentioned a geographical criterion.

(2) With regard to access, the CJEU followed the same logic as with retention and reiterated that access to retained data must correspond genuinely and strictly to the (exhaustive list of) objectives referred to in Art. 15(1)[35] stressing that only the objective of fighting serious crime is capable of justifying access to retained data.[36] Furthermore, the CJEU recalls that legislation governing access to retained data needs to strictly comply with the proportionality principle,[37] i.e. it must not exceed the limits of what is strictly necessary. The CJEU outlined that such legislation must lay down clear and precise substantive and procedural conditions governing the access to the retained data.[38] Specifically, the legislation needs to be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities may be granted access.[39] This means that in the context of fighting crime, as a general rule, access may be granted only to the data of individuals suspected of planning, committing or having committed a serious crime or of being otherwise implicated in such crime. However, the CJEU also hinted to an exception by adding that in particular situations, where vital national interests are at stake, e.g. threats of terrorist activities, access to data of other persons might be granted, provided there is objective evidence that that data might, in a specific case (in other words, in that exceptional case), make an effective contribution to combating such activities. The CJEU nonetheless clarified that general access to all retained data, irrespective of any links or connections with the intended purpose, cannot be regarded as strictly necessary, hence it is disproportionate.[40]

The CJEU stressed that prior review by a court or an independent administrative body of the request for access by the competent authority is required, in order to ensure full respect for the necessary conditions and procedures outlined – this necessity for review also follows directly from Art. 8(3) of the Charter, although still leaving room for exceptions in urgent cases.[41] The CJEU further demanded a notification of the persons affected, once such notification no longer jeopardises the investigations undertaken.[42] In addition, the CJEU clarified that Art. 15(1) of the e-Privacy Directive does not provide for a derogation with respect to the rules relating to security and protection of the data. This requires that providers guarantee a particularly high level of protection and security, that the data is retained within the EU and that data is irreversibly destroyed at the end of the retention period.[43] Whether and to what extent the national legislation reviewed by the CJEU in *Tele2/Watson* satisfied the established requirements from Art. 15(1) read in the light of Arts. 7, 8, 11 and 52(1) of the Charter was however left for the referring court to determine. This is somehow unsatisfactory, but inevitable as the CJEU has to limit itself to its function under Art. 267 TFEU and the questions referred to it.

In *Tele2/Watson*, the CJEU ultimately shed light on the scope of the e-Privacy Directive. This has been a much-debated question and several Member States had expressed doubts as to the applicability of that Directive in the context of Member States' security measures. The CJEU held that national legislation governing the obligation of providers of electronic communication services and networks to retain traffic and location data as well as rules on access to such data by competent national authorities fall within the scope of the e-Privacy Directive, even if the sole objective of such legislation was to combat crime alone. Such legislation thus needs to be measured against the Charter.[44] The protection of the confidentiality of electronic communication and related traffic data guaranteed by that Directive applies to the measures taken by all persons (other than the users), no matter whether private persons or bodies or State bodies.[45] Legislative measures, which, pursuant to Art. 15(1) of the e-Privacy Directive, restrict the scope of the rights and obligations provided in the e-Privacy Directive, cannot be considered "activities of the State" within the meaning of Art. 1(3) of the e-Privacy Directive, no matter if the objectives to be pursued under Art. 15(1) and the objectives referred to in Art. 1(3) overlap.[46] Referring to the structure of the e-Privacy Directive and the purpose of its Art. 15, the CJEU stressed that Member States may only adopt restrictive legislative measures, on condition that they comply with the prerequisites laid down in that very Article.[47] Accordingly, this applies to legislative measures that require providers to retain traffic and location data, as well as measures governing the access by national authorities to the retained data, since both issues include processing activities by the providers.[48] This means that the retention of data and access to such data must be considered like two sides of the same coin and both fall within the scope of the e-Privacy Directive.

3. Interim conclusion

The CJEU's jurisprudence in *Digital Rights* and *Tele2* set the threshold very high. It is a benchmark against which the CJEU is going to review later preliminary ruling requests brought on this matter. At the same time, it should be stressed that the CJEU has not dismissed data retention as such in both judgments. Even more, the CJEU considered the retention of data and access thereto by national authorities a suitable tool that has an added value in combating serious crimes, however, without specifying further how it reaches such conclusion. To that end, the CJEU left room for possible forms of data retention from the beginning, giving ample advice on what such solutions could look like.

At the same time, despite the clear language of the CJEU in *Digital Rights* and *Tele2*, there was no coherent understanding at the national level as to how these judgements and their consequences should be interpreted. At least, there seemed room for interpretation. In 2017, for instance, the Constitutional Court of Portugal found that the declaration of invalidity of the data retention Directive did not have an automatic consequence on the validity of a national law transposing it. Moreover, it found that Portugal introduced an extensive and complex framework, including on access to and protection of retained data, which goes far beyond the invalid data retention Directive and the CJEU's jurisprudence, and that these specificities have to be looked at in their entirety and could not be disregarded when assessing certain provisions on data retention. The Constitutional Court of Portugal hence declared the retention of subscriber information with respect to dynamic IP addresses on the basis of the Portuguese Law as constitutional.[49] The Council of Ministers of Belgium argued a year later in a similar way in proceedings before the Constitutional Court (*Cour Constitutionelle*) of Belgium.[50]

Overall, a large number of Member States did not see a compelling need to fundamentally change their national laws and, in effect, the previous practice remained in place as before.

III. Recalibrating Data Retention in the EU – The CJEU's Decisions in the Cases *Privacy Int., Quadrature du Net et al., Ordre des barreaux* and *H.K. v Prokuratuur*

Following the *Tele2* decision, the rules governing the activities of national intelligence agencies came more and more into the focus of national courts in several Member States. Although the CJEU in *Tele2* also scrutinised the Swedish Law on gathering of data relating to electronic communication as part of intelligence gathering by law enforcement authorities,[51] national courts generally expressed doubts that the strict line taken by the CJEU in its previous decisions with regard to the retention of data and the access thereto could be applied to the sensitive activities of national intelligence agencies. Requests for preliminary ruling were thus made by the Investigatory Powers Tribunal in the United Kingdom,[52] the French Conseil d'Etat[53] and the Belgian *Cour Constitutionelle*[54], which the CJEU took a stance on in two comprehensive judgements of 6 October 2020. Shortly thereafter, on 2 March 2021, the CJEU shed more light on this matter in a request for preliminary ruling submitted by the Supreme Court of Estonia.[55]

1. Facts of the cases in *Privacy Int., Quadrature du Net, Ordre des barreaux francophones and germanophone et al.*

The UK request in the case *Privacy International* concerned the transfer of bulk communication data from providers of public communications networks, under the directions issued

by the UK Secretary of State, to national security and intelligence agencies, where that data was used by those agencies, in particular by way of automated processing. This practice is said to have been going on for almost two decades. The referring court highlighted the importance of using bulk communication data by security and intelligence agencies for the protection of national security, including counter-terrorism, counter-espionage and counter-nuclear proliferation, and found that this practice was also compliant with the ECHR. It hence sought to clarify whether, and if so to what extent, EU law and in particular the e-Privacy Directive, was applicable, given that according to Art. 4(2) TEU and in view of Art. 1(3) of the e-Privacy Directive, national security remains the sole responsibility of the Member States.[56]

The French and Belgian requests in *Quadrature du Net* and *Ordre des barreaux francophones and germanophone et al.* concerned a wide range of questions surrounding the newly adopted data retention regimes in place in France[57] and Belgium[58] respectively. The Belgian legislation envisaged a general and indiscriminate retention of traffic and location data for a period of 12 months and allowing access thereto by various national authorities, e.g. police and judicial authorities, intelligence and security authorities as well as emergency call services and authorities responsible for missing persons. The motifs of that legislation state that it is impossible to know in advance which data is needed and that it is equally impossible to limit the retention of data to certain groups of persons, to include time limits or to restrict the retention to geographic areas.[59] In the proceedings before the *Cour Constitutionelle* it was even stated that a "targeted retention", as suggested by the CJEU in *Tele2*, could easily lead to or be perceived as discrimination.[60] The Belgian Constitutional Court hence asked, first, whether a general data retention obligation, which is provided with certain safeguards on storage and access, was compatible with EU law and in particular Art. 15(1) of the e-Privacy Directive and Arts. 7, 8 and 52(1) of the Charter, taking into account that the aim of the legislation was not limited to fighting serious crime but also intended to safeguard national security, defence, public security, and to prevent, investigate, detect and prosecute other criminal offences. The Belgian Constitutional Court then reverses the perspective and asks in its second question whether general data retention may be duly justified if the objective is to enable the state to fulfil its positive obligations under Arts. 4 and 7 of the Charter, thus, ensuring the effective criminal investigation and effective punishment of perpetrators of sexual abuse of minors, when they made use of electronic communication means. The Constitutional Court finally asks whether, in the event that the CJEU finds the data retention legislation under review as incompliant with EU law, the consequences of that legislation could be maintained, in order to enable the further use of previously stored data, so as to avoid legal uncertainty.

Similarly, the French requests concerned legislation adopted after the *Charlie Hebdo* and *Bataclan* terrorist attacks. The legislation envisaged gathering intelligence related to protecting and promoting a set of State interests, such as national independence, integrity, defence, and prevention of terrorism or organised crime as well as certain foreign policy, economic, industrial and scientific interests. The referring French court sought clarity as to whether a general and indiscriminate retention for such purposes may be justified by the right to security guaranteed by Art. 6 of the Charter, thereby also highlighting that national security falls within the sole responsibility of the Member States pursuant to Art. 4(2) TEU. It also inquired about the compliance with EU law of special measures for the purpose of preventing terrorism, such as real-time collection of traffic and location data and automated data processing, which, as the referring court noted, would not impose any specific retention obligations on the providers of communication and network services. The referring court lastly sought clarity in relation to the collection of metadata, namely whether it is a prerequisite for the collection that the data subjects are notified of the measures.

2. Key findings of the CJEU

In the judgments deciding the three cases, the CJEU generally follows the line of argument taken in its previous decisions. However, it also opened the door to a number of important exceptions in very elaborate and concrete terms. If one were to sum up the previous decisions as to say that data retention was overall prohibited unless it is allowed in certain situations, the impression now is that data retention may be more widely used, as long as it is not excessive (in particular if one reads the *Quadrature du Net* judgment). The following analyses in detail the judgments in *Privacy Int.* and *Quadrature du Net et al.* underpinning this hypothesis.

a) Clarifying the scope of the e-Privacy Directive

At first, the CJEU reconfirmed its established argument taken in *Tele2* regarding the scope of the e-Privacy Directive. National measures do not fall outside the scope of the Directive just because they have been taken for the purpose of protecting national security.[61] The CJEU stressed that such measures need to comply with the prerequisites laid down in Art. 15(1), both, in respect of retaining data as well as access thereto and cannot be considered "activities of the State" within the meaning of Art. 1(3), no matter if the objectives to be pursued under Art. 15(1) and the objectives referred to in Art. 1(3) of the e-Privacy Directive overlap.[62]

Art. 4(2) TEU does not change this conclusion. The CJEU acknowledged, in line with its earlier jurisprudence, that it is

for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security.[63] However, it holds that the mere fact that a national measure has the purpose of protecting national security cannot render EU law, such as the e-Privacy Directive, inapplicable and exempt the Member States from their obligation to comply with that law.[64] These findings also apply to the special case of the UK request, where the CJEU dismissed the argument that the transfer of the entire data to intelligence authorities by the service and network providers was to be considered mere technical assistance to an act carried out solely by the State to protect national security, as stipulated in Art. 4(2) TEU.[65]

The CJEU also clarified that nothing else follows from its judgement in Case *Parliament v Council and Commission,*[66] where the CJEU held in the context of Passenger Name Records (PNR) that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes fell outside the scope of the data protection Directive 95/46.[67] Although Art. 1(3) of the e-Privacy Directive, which excludes from the scope of that directive, in a similar manner as Art. 3(2) of Directive 95/46 did in the past, activities concerning public security, defence and State security, the comparison with the case on PNR does not hold in the CJEU's view. According to the CJEU, the wording of Art. 3(2) of Directive 95/46, was broader and excluded in a general way processing operations concerning public security, defence and State security from its scope, regardless of who is carrying out the data processing operations.[68] By contrast, Art. 1(3) of the e-Privacy Directive, as the CJEU points out, makes a distinction as to who carries out the data processing operation concerned with all processing operations by providers of communication services, including processing operations resulting from obligations imposed by the public authorities, falling within the scope of the e-Privacy Directive.[69]

Moreover, Directive 95/46 was repealed by Regulation 2018/679 (the General Data Protection Regulation – hereinafter "GDPR") and although Art. 2(2)(d) GDPR envisages that processing operations by "competent authorities" for the purpose of, *inter alia*, prevention and detection of criminal offences are not covered by that Regulation, Art. 23(1)(d) and (h) GDPR makes it clear that processing of personal data carried out by individuals clearly falls within the scope of that Regulation. The interpretation of the e-Privacy Directive, which supplements and further specifies the GDPR, is insofar consistent.[70] The CJEU states that only measures that are directly implemented by national authorities fall outside the scope of the e-Privacy Directive and have to be assessed on the basis of national (constitutional) law and the ECHR.[71]

Overall, the CJEU follows a narrow interpretation of Art. 4(2) TEU, which does not leave much room outside the scope of EU law. The CJEU draws a very fine line between its judgement on *PNR* on the one hand and its judgements in *Privacy Int.* and *Quadrature du Net* on the other. The CJEU did not (have to) elaborate in its *PNR* decision on the differences in the wording and the scope of Art. 3(2) of Directive 95/46 and Art. 1(3) of the e-Privacy Directive, respectively; this point was highlighted only later in the *Quadrature du Net* decision, more concretely, in the opinion provided by Advocate General Campos Sánchez-Bordona.[72] In its *PNR* decision, the CJEU essentially based its findings on the point that although the PNR data was collected by private operators for commercial purposes and subsequently transferred by them to a third country, Art. 3(2) of Directive 95/46 still applied and (hence) that the actual transfer of data fell outside the scope of that Directive. The transfer fell, instead, within a framework established by the public authorities that related to public security.[73] It begs the question whether the CJEU would indeed have decided on *PNR* today in the same way as it did in 2006, in view of its approach it has taken most recently.

b) Reconfirming the preclusion of a general and indiscriminate retention of traffic and location data

The CJEU then reconfirmed its established line that EU law precludes national legislation that prescribes a general and indiscriminate retention as well as a transmission of traffic and location data.[74] This also applies in respect of security and intelligence agencies for the purpose of safeguarding national security.[75] Thereby, the CJEU closely followed its systematic approach developed in *Tele2.* It reiterated the principle of confidentiality of traffic and location data protected under the e-Privacy Directive and the safeguards, which apply in the case of an exceptional derogation based on Art. 15(1), in particular the strict compliance with the rights enshrined in the Charter. The CJEU identified Arts. 7, 8 and 11 of the Charter as the fundamental rights affected, without actually defining in detail the scope of protection of these rights. The CJEU pointed out, however, that the protection under the e-Privacy Directive directly emanates from the rights enshrined in Arts. 7 and 8 of the Charter.[76]

It stressed that the retention in itself constitutes an interference with those fundamental rights, irrespective of whether such data is sensitive, harmful to the persons concerned or whether such data has actually been used subsequently.[77] It also flagged the potential risks of abuse and unlawful access resulting from the significant quantity of traffic and location data retained under a general and indiscriminate retention measure.[78] In line with Art. 52(1) of the Charter, the CJEU examined whether, and if so to what extent, the limitations on the fundamental

rights affected caused by the measures under review are justified, in particular, whether such measures are proportionate and meet the objectives of general interests recognised by the Union or the need to protect the rights and freedoms of others.

Accordingly, the CJEU turned to the question, as specifically requested by the referring courts, whether any positive obligations flowing from Arts. 3, 4, 6 and 7 of the Charter, could demand the adoption of measures, such as those under review, which could be in conflict with Arts. 7, 8 and 11 of the Charter and accordingly Art. 15(1) of the e-Privacy Directive in the present cases.

With regard to the right to security of person in Art. 6 of the Charter, the CJEU makes reference to the ECtHR case law on the corresponding Art. 5 ECHR.[79] The CJEU clearly dismissed the idea put forward by the referring courts that Art. 6 of the Charter could impose any sort of positive obligations on the State to take specific measures to prevent and punish certain criminal offences,[80] which would justify the derogation from the principle of confidentiality under the e-Privacy Directive.

The CJEU was however more susceptible to potential positive obligations deriving from Art. 3 (right to the integrity of the person), Art. 4 (prohibition of torture and inhuman or degrading treatment or punishment), and Art. 7 (respect for private and family life) of the Charter.[81] Without defining the scope of application and the width of these rights, the CJEU just made reference to the jurisprudence of the ECtHR on Arts. 3 and 8 ECHR, which correspond to Arts. 4 and 7 of the Charter, and stated that the rights require the putting in place of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against a person through effective investigation and prosecution – this in particular, when a child's physical and moral well-being is at risk.[82] To that end, the CJEU concluded that, as the ECtHR found, a legal framework should be established allowing to strike a balance between the various interests and rights to be protected.[83] The CJEU did, however, not go into greater detail or elaborate on the scope of any of these positive obligations and to what extent they themself are subject to limitations.

With regard to proportionality, the CJEU reiterated that derogations from and limitations on the protection of personal data must apply only insofar as they are strictly necessary and that the objective pursued must be proportionate to the seriousness of the interference.[84] This requires the laying down of clear and precise rules on the scope and application of the measure in question and ensuring minimum safeguards. In particular, the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued.[85]

c) Recalibrating data retention – exceptions to the strict rule followed by the CJEU hitherto

While the CJEU in *Tele2* opened a crack in the door for a data retention regime that would satisfy the CJEU's strict requirements by introducing the concept of a "targeted retention", it now widely opened the door in the *Quadrature du Net* decision for a variety of possible exceptions to its established rule that a general and indiscriminate retention of traffic and location data is precluded. Building on the approach, line of arguments and caveats developed in *Tele2*, the CJEU underlined that the different objectives referred to in Art. 15(1) of Directive 2002/58 as well as the types of personal data demand differentiation as regards the potential limitations to the principle of confidentiality of personal data. Moreover, there is a need to strike a balance between the rights and the interests at issue depending on the circumstances of the case. The CJEU elaborated on the various types of scenarios and exceptions, one by one:

■ Legislative measures for the purpose of safeguarding national security

The first and presumably the most far-reaching and significant exception concerns measures providing for the preventive retention of traffic and locations data for the purpose of safeguarding national security. The CJEU stressed that the objective of safeguarding national security has not yet been specifically examined by it, although it already clearly hinted to a different treatment of measures for the purpose of safeguarding national security in particular situations in *Tele2*.[86]

Briefly and without much ado, the CJEU went back to Art. 4(2) TEU – which it dealt with in detail in the context of reviewing the scope of application of EU law for measures that serve the purpose of protecting national security (see above a)). It now recalls that national security remained the sole responsibility of Member States and that that responsibility corresponds to the primary interest to protect the essential functions of the State and the fundamental interests of the society. This responsibility entails the ability to prevent and punish activities which could seriously go against these interests. By way of an example the CJEU mentioned terrorist activities.[87] As already pointed out in *Tele2,*[88] the CJEU set out that the objective of safeguarding national security is different from the other objectives referred to in Art. 15(1) of the e-Privacy Directive. Outlining that threats to national security are different by their nature and particularly serious, the CJEU concluded that the objective of safeguarding national security is hence capable of justifying measures that entail a more serious interference with fundamental rights, provided that the other requirements as laid down in Art. 52(1) of the Charter are met.[89] To this end, the CJEU did not mention any potential positive obliga-

tions that could be derived from the fundamental rights that the CJEU itself had identified in this context and that could potentially demand justifying such exception.

On that basis, the CJEU concluded that, as long as there are sufficiently solid grounds that a Member State is confronted with a serious threat to national security, which is genuine and present or foreseeable, Art. 15(1) of the e-Privacy Directive read in light of the Charter does not preclude legislative measures which permit ordering the providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time. Although the CJEU still echoed the principles it had established in its previous jurisprudence, such as that the instruction to retain must be limited in time to what is strictly necessary, it clarified that the instruction may be renewed for a foreseeable period of time, however, stressing that the retention cannot be systematic in nature. To that end, the instructions to providers of electronic communications services have to be subject to effective review by a court or an independent administrative body, which needs to verify that one of the situations justifying the general and indiscriminate retention actually exists and that the conditions and safeguards are observed.[90]

Legislative measures for the purpose of safeguarding public security (criminal offences)

As regards legislative measures for the purpose of safeguarding public security, that is preventing, investigating, detecting and prosecuting criminal offences, the CJEU followed its systematic approach in *Tele2* (see above); however, it shed more light on possible exceptions, in particular on its concept of "targeted retention". It reiterated that, based on the principle of proportionality, only the objective of fighting serious crime and measures to prevent serious threats to public security are capable of justifying an interference such as the retention of traffic and location data. The CJEU clarified that even positive obligations, which might flow from Arts. 3, 4, and 7 of the Charter, as outlined above, cannot justify an interference that is as serious as the retention of traffic and location data without any restrictions and without a connection between the data of the persons concerned and the objective pursued.

This is different, as the CJEU pointed out, in the case of a "targeted retention", provided it is designed in a way that the legislation envisaging the retention of traffic and location data is limited to what is strictly necessary with respect to the categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted. The choice must be based on objective and non-discriminatory factors.[91] The CJEU also considered that a targeted retention for the purpose of combating serious crimes or preventing serious threats to public security would be justified, *a fortiori*, for the purpose of safeguarding national security. In other words, what suffices for the less serious purpose, also suffices for the graver one.

Preventive retention of IP addresses and data relating to civil identity to combat crime and safeguarding public security

The third exception concerns, in essence, ways and means to identify the users of electronic communications systems, i.e. the retention of IP addresses and data relating to civil identity. The CJEU stated that IP addresses mainly help identify the natural person who owns the device from which an internet communication is made.[92] Provided that only IP addresses of the source and not the IP addresses of the recipient of the communication are retained, the CJEU considered this category of data as being less sensitive than other traffic data.[93]

Nonetheless, since IP addresses may be also used, beyond determining the terminal equipment utilised, to track the user's clickstream, thus, the entire online activity and hence establish a detailed profile of the user, the retention would constitute a serious interference with Arts. 7, 8 and 11 of the Charter.[94] The CJEU noted, however, that for the detection of criminal offences committed online, the IP address might be the only possibility to identify the person to whom that IP address was assigned at the time of the commission of the offence. Without retaining the IP address, the detection of offences committed online – the CJEU specifically mentioned serious child pornography offences in this context – may prove impossible.[95]

The CJEU conceded that a retention of IP addresses of all natural persons who own terminal equipment permitting access to the internet would include also those, who "at first sight"[96] have no connection with the objectives pursued.[97] Notwithstanding, the CJEU concluded that "in those circumstances"[98] the general and indiscriminate retention of IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Art. 15(1) of the e-Privacy Directive read in light of the Charter – provided that it is subject to strict compliance with substantive and procedural conditions. This means that such retention may be only used to combat serious crimes or to prevent serious threats to public security – and *a fortiori* also to safeguard national security. The retention period must not exceed what is strictly necessary, while conditions and safeguards on the use of the data, particularly as regards tracking, need to be in place and strictly objective.

In the same context, the CJEU reconfirmed its previous jurisprudence as regards data relating to the civil identity of users of

electronic communication systems and developed its approach further. It maintained its line that such data only provides contact details of the user, such as the name and the address, and that it neither concerns the date, time, duration or frequency of the communication, nor the recipients of the communication or the location where the communication took place. The CJEU held that data relating to the civil identity does not contain any information on the communications sent and hence on the user's private life.[99] Although the retention of such data constitutes an interference with Arts. 7 and 8 of the Charter, this interference cannot be considered to be serious, according to the CJEU. Thus, such non-serious interference may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general.[100] While in *Ministerio Fiscal*[101] the CJEU only ruled on the question of access to such data,[102] it looked in *Quadrature du Net* at the question of the retention of such data in itself and concluded, after striking a balance between the conflicting interests,[103] that Art. 15(1) of the e-Privacy Directive read in the light of the Charter does not preclude legislative measures requiring providers of electronic communication services to retain data relating to the civil identity of all users for the purpose of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security. Although such retention may be justified with the objective of preventing or combating any criminal offence,[104] the CJEU held that there is not even a necessity for a connection between the retained data on civil identity of all the users and the objectives pursued.[105] Furthermore, the CJEU stated that there is no specific time limit for such retention,[106] while it remained entirely silent on the question of judicial review.

■ Legislative measures providing the expedited retention of traffic and location data for the purpose of combating serious crime ("quick freeze")

The next exception concerns cases of expedited retention of traffic and location data for the purpose of combating serious crime, sometimes also referred to as "quick freeze". In these situations, the data has been already stored by the service providers, e.g. for billing, traffic management or value added services.[107] As that data needs to be erased or made anonymous after a certain period of time to comply with the principle that the storage does not exceed the limit of what is strictly necessary, competent authorities may order an expedited preservation of such data in order to preserve it for the purpose of investigating criminal offences or acts adversely affecting national security. This is pertinent, according to the CJEU, only in situations, where these offences or acts have been already established or where such offences and acts may reasonably be suspected.[108] The CJEU referred to the Council of Europe Convention on Cybercrime,[109] which envisages the adoption of measures, such as the expedited preservation of traffic data, for the purpose of criminal investigations, where there are grounds to believe that that data may be lost or modified.[110]

Given the serious interference with fundamental rights, which such retention would entail, only actions to fight serious crime and, *a fortiori*, safeguarding national security may be justified.[111] Moreover, when balancing the rights and interests at issue, the CJEU stressed that under Art. 8(2) of the Charter the processing of data must be consistent with its specified purpose, while the purpose for retaining data in the case of the expedited retention (fighting crime) might not or no longer correspond to the purpose for which the data was initially processed and stored (e.g. billing). The CJEU held that it is permissible to adopt legislation under Art. 15(1) of the e-Privacy Directive, which provides for the possibility of an expedited retention, whereby competent authorities[112] may instruct providers of electronic communication services to undertake an expedited retention of traffic and location data for a specified period of time.[113] However, such legislation must clearly set out for what purpose such expedited retention may be requested, while the instruction decision shall be subject to judicial review.[114] To comply with the principle of proportionality, the retention must relate only to traffic and location data that may shed light on serious crimes or acts affecting national security, while the retention period must be limited to what is strictly necessary (however, if necessary, the retention period may also be extended).[115] Despite the limitation to what is strictly necessary, this leaves some interpretative room; the CJEU further widened the scope of this exception by stating that the data does not need to be limited to the persons specifically suspected of the crimes or the act in question but also to other persons or geographic areas, provided that on the basis of objective and non-discriminatory factors such data can shed light on the offences or acts in question.[116] It is of particular note that, according to the CJEU, the exception of an expedited retention may be combined with another exception justified under Art. 15(1) of the e-Privacy Directive, e.g. in situations where the time period of a measure is due to expire that data may be preserved beyond that period by way of the expedited retention. This opens up for a great degree of flexibility and wider use of the measures under Art. 15(1).[117] Access to such data is granted following the general principles on access, as established in *Tele2*.[118]

■ Legislative measures providing for an automated analysis and real-time collection of traffic and location data for the sole purpose of preventing terrorist activities

Beyond the general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security, which the CJEU exceptionally considered justified under cer-

tain strict conditions,[119] it also had to review legislation that concerned certain preventive intelligence gathering techniques used in situations of serious threats to national security: the automated analysis and real-time collection of traffic and location data, as well as the real-time collection and transmission of technical data concerning the location of terminal equipment.

The automated analysis envisages a screening at the request of competent national authorities of all traffic and location data carried out by providers of electronic communication services against previously set parameters.[120] This covers all traffic and location data of all users of electronic communication systems and constitutes a processing of data with the assistance of an automated operation within the meaning of Art. 4(2) GDPR.[121] This processing is also independent of the subsequent collection of data of persons identified following the automated analysis. The CJEU pointed out that this intelligence gathering technique is likely to reveal the nature of the information consulted online and is conceived so as to apply generally to all persons, including to those, where there is no evidence that their conduct is linked in any way with terrorist activities. The CJEU concluded that this processing constitutes a particularly serious interference with Arts. 7, 8 and 11 of the Charter.

To justify such particularly serious interference in accordance with Art. 52(1) of the Charter, the CJEU fetched the requirements it established in the context of the legislative measures for the purpose of safeguarding national security (see above), stressing that the automated analysis of traffic and location data may only be considered as proportional in situations in which a Member State is facing a serious threat to national security which is genuine and present or foreseeable and provided that the duration is limited to what is strictly necessary.[122] The decision authorising automated analysis must be subject to review by a court or an independent administrative body, which verifies whether the situation justifying that measure exists and whether the conditions and safeguards that must be laid down by legislation are observed.[123] Given the specificities of the automated analysis, the underlying models and criteria for the automated analysis must be determined in a non-discriminatory manner,[124] and any positive result obtained from such analysis requires an individual re-examination by non-automated means before the person concerned is adversely affected by a subsequent measure, such as a real-time collection of his/her traffic and location data.[125] Generally, the CJEU saw a need for regular re-examinations of the pre-established models and criteria to ensure that they are up-to-date and non-discriminatory and limited to what is strictly necessary.[126] The CJEU left open who should carry out such examination and at which frequency.

The CJEU's review of the real-time collection of traffic and location data generally builds upon the automated analysis. It may be individually authorised in respect of a person or persons belonging to the same circle previously identified through the automated analysis as potentially having links to a terrorist threat.[127] Such processing allows for continuous monitoring and in real-time – for the period of time authorised – of the person(s), the means and duration of communication, the place of residence and movements of that/these person(s) and may also reveal the information consulted online. The legislation under review in *Quadrature du Net* envisaged also the possibility to collect the technical data concerning the location of the device used and transmit it in real-time to a department reporting to the Prime Minister.[128]

The CJEU noted that such measure constitutes a derogation from Art. 15(1) of the e-Privacy Directive and an interference with Arts. 7, 8, and 11 of the Charter, stressing that the real-time collection and transmission of data that allows a real-time location of the device used is particularly serious, amounting to virtually a total monitoring of the persons(s) concerned. Such real-time access is more intrusive than a non-real-time access.[129]

The CJEU held that this measure, which aims at preventing terrorist activities, and which complements the automated analysis and the exceptional general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security (see above), may be justified only in respect of persons for whom there is a "valid reason to suspect" that they are involved "in one way or another in terrorist activities."[130] Persons, who do not fall into this category, e.g. who are potentially involved in serious crimes but not terrorist activities, might fall into one of the other exceptions described by the CJEU (see above).

The decision authorising such real-time collection must be based on objective and non-discriminatory criteria provided for in national legislation. It must be subject to prior review by a court or an independent administrative body, which needs to check whether the conditions are observed, in particular whether the real-time collection is limited to what is strictly necessary.[131]

In this context, the question arose whether the person(s) concerned by these intelligence gathering measures need to be notified and whether such notification is a prerequisite for the compliance with the requirements under Art. 15(1) of the e-Privacy Directive.[132] The French law in question did not envisage a notification. Instead, it provided for the possibility for any person to file a complaint with the Commission for the Oversight of Intelligence Techniques; this Commission verified that no intelligence techniques have been unlawfully implemented against the complainant.[133] The Commission subse-

quently notified the complainant that it assessed the complaint, however, it neither confirmed nor denied that an intelligence gathering technique was applied against the complainant.[134] The complainant then could seek recourse before a special panel of the *Conseil d'Etat*, which investigated the complaint and, could request the competent authorities to remedy illegalities found.[135] According to the referring French court, this complaint mechanism satisfied the requirements under Art. 15(1) read in light of the Charter.[136]

Contrary to the views expressed by the referring French court, the CJEU held that the person affected by a real-time collection of traffic and location data needs to be notified.[137] This is necessary to enable the person to exercise his/her rights under Arts. 7 and 8 of the Charter, i.e., to request access to the data that has been subject of the measures and to request rectification or erasure, if necessary.[138] The requirement to notify also follows from Art. 47 of the Charter, which guarantees the right to an effective remedy before a tribunal, a right explicitly mentioned in Art. 15(2) of the e-Privacy Directive, read in conjunction with Art. 79(1) GDPR.[139] As for the automated analysis, which is applied generally to all persons, the CJEU held that the competent national authority needs to publish information of a general nature relating to the analysis, without having to notify each and every person individually. However, once a person has been identified on the basis of the models and criteria of the automated analysis, it is necessary to notify that person individually. The CJEU stressed, however, that the notification must take place only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which the authorities are responsible.[140]

d) Access by competent national authorities

In its recent decisions, the CJEU mainly elaborated on the various exceptions it established as far as the retention of traffic and location data is concerned. As regards an authority's access to such data, the CJEU primarily reiterates its findings in *Tele2* (see above II.); however, it also provides greater clarity on its jurisprudence and develops it further.

■ Greater clarity on the CJEU's strict line on access to retained data

Alas, following the line taken in *Tele2*, the CJEU stressed that access may be justified only by the public interest objective, for which the providers were ordered to retain the data, and must comply with the principle of proportionality.[141] To dispel any doubts, the CJEU stressed in particular that access to data for the purpose of prosecuting and punishing an ordinary criminal offence may not in any event be granted where the retention of that data has been justified by the objective of combating serious crime or safeguarding national security.[142] However, similarly as for the retention for the purpose of combating crime and safeguarding public security, the CJEU followed the logic that what suffices for the less serious purpose, also suffices for the graver one. This means that access to data, which was retained for the purpose of serious crime, may also be justified if access is sought for the purpose of safeguarding national security.[143]

This underlines the independence of and inter-dependence between the retention and the subsequent access thereto – independence because the CJEU checks the validity of the retention and the access for each independently and inter-dependence because both are linked with and have an impact on each other. Generally, as outlined in *Tele2,* prior review by a court or an independent administrative body of the reasoned request for access by the competent authority is mandatory in order to ensure full respect of the necessary conditions and procedures outlined.[144]

The CJEU also shed more light on cases of duly justified urgency, where it holds that the review by a court or independent administrative body needs to take place quickly but not necessarily before accessing the data.[145] The CJEU, however, did not elaborate in greater detail on what constitutes such due justification and how access should be granted in the absence of a prior (authorising) decision.

Finally, the CJEU also clarified that these requirements also apply to the particularly invasive automated analysis and real-time collection of traffic and location data;[146] in particular, a court or an independent administrative body needs to check whether the conditions are fulfilled, and the measure is limited to what is strictly necessary.

■ Proportionality considerations on access and flawed retention – case HK v Prokuratuur

The inter-dependence between retention and subsequent access to traffic and location data, referred to above under aa) was also illustrative in the CJEU's most recent decision on a request for preliminary ruling by the Supreme Court of Estonia.[147] This request concerned criminal proceedings against a person found guilty of the commission of petty crimes and acts of violence,[148] where the question arose whether Art. 15(1) of Directive 2002/58 read in light of the Charter precludes national legislation that permits public authorities to obtain access to a set of traffic and location data for the purpose of preventing, investigating, detecting, and prosecuting criminal offences that were not limited to serious crimes, even if the access granted was short and the type of data accessed limited. The Estonian legislation in question envisaged a general and

indiscriminate retention of traffic and location data related to fixed and mobile telephony for one year. Access thereto could be requested in relation to any type of criminal offence.[149] The data obtained in such way was constitutive for the conviction in the main trial in the case at issue.

The CJEU reiterated that access may be granted only insofar as the data was retained in a manner consistent with Art. 15(1),[150] thereby referring to its jurisprudence on the preclusion of a general and indiscriminate retention of traffic and location data.[151] In that sense, access may be justified only by the public interest objective for which the providers of electronic communication services were ordered to retain the data[152] and provided it is proportionate to the seriousness of the interference with Art.15(1) of Directive 2002/58 read in light of Arts. 7, 8 and 11 of the Charter.[153]As outlined in its earlier jurisprudence, the CJEU stressed that only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying a serious interference with fundamental rights, such as the retention of traffic and location data, no matter whether the retention is general and indiscriminate – as in the case under review – or targeted.[154]

Accordingly, access to a set of traffic and location data is justified only by the objective of combatting serious crime or prevent serious threats to public security.[155] The CJEU clarified that nothing changes if account is taken of factors related to the proportionality of the request for access, such as the length of the period in respect of which access to such data is sought or a narrow scope of the categories of data covered, because these factors cannot justify from the outset that access is granted in pursuance of the objective of preventing, investigating, detecting and prosecuting criminal offences in general.[156] The interference with fundamental rights in the case under review is and remains serious which may be only justified by pursuing the objective to prevent or investigate serious crimes, rather than crimes in general. In the case at issue, the access failed already at the first step, while subsequent considerations of the proportionality of the access are insofar irrelevant.

■ What does (not) constitute a court or independent administrative body?

In *HK v Prokuratur*, the CJEU ultimately had to take a stance on the question of what constitutes a "court or independent administrative body" within the meaning of its jurisprudence on data retention. The question was whether Art. 15(1) of the e-Privacy Directive read in light of the Charter precludes national legislation that confers on the public prosecutor's office the power to authorise access to traffic and location data for the purpose of criminal investigations.[157] The referring Estonian Supreme Court stated that, under national law, the public prosecutor's office, which is hierarchically organised, is obliged to act independently and is subject only to the law. It examines incriminating and exculpatory evidence in the pre-trial procedure and represents the public prosecution at the main trial, thus it is a party to the proceedings. There are, however, no formal requirements to access the desired data and, in effect, the prosecutor may make a request for access himself in a case.[158]

It is not surprising that the CJEU set an end to this practice. It recalls that national legislation adopted pursuant to Art. 15(1) needs to lay down the substantive and procedural conditions governing the access by the competent national authorities to traffic and location data retained by providers of electronic communications services and must comply with the principle of proportionality.[159] Such legislation must provide for clear, precise and objective rules governing the scope and application of the measure and impose minimum safeguards to effectively protect against the risk of abuse. Above all, a general access to all retained data cannot be regarded as being limited to what is strictly necessary.[160]

The court or an independent administrative body entrusted to carry out the review of the reasoned request for access must have all the power and provide all the necessary guarantees to reconcile the various interests and rights at issue.[161] The CJEU indicated that the independent administrative body must have the status enabling it to act objectively and impartially when carrying out its duties and must be free from any external influence.[162] The requirement of independence of the court or body means that it has to be different from the authority that makes the request in order to review the matter objectively and impartially and free from any external influence. This means in particular that the court or body must not be involved in the conduct of the criminal investigations in question and has to be neutral vis-à-vis the parties to the criminal proceedings. These requirements are not fulfilled in the case of a public prosecution office, irrespective of its independent status under national law.[163] Although not congruent, it is to be seen how this jurisprudence will be reconciled with the CJEU's jurisprudence on the status of a public prosecution office as a judicial authority for the purpose of issuing European Arrest Warrants.

e) Consequences of a potentially unlawful retention of or access to data used as evidence in criminal proceedings

Having elaborated extensively on the various rules and exceptions of a data retention regime, the CJEU had to address the question on the consequences of a potential unlawful retention of or access to traffic and location data that was used as evidence in criminal proceedings. This question was put forward by the Belgian *Cour Constitutionelle.*[164] Concretely, the refer-

ring Belgian court sought to address that issue by inquiring whether it may maintain the effects – at least temporarily – of the national law on data retention under review, even if the CJEU has found that it does not comply with EU law.[165] The *Cour Constitutionelle* states that maintaining the effects would allow national authorities to continue using the previously collected and retained data, primarily for the purpose of criminal proceedings, thus avoid legal uncertainty.[166] This would mean that legislation would continue to impose obligations on providers of electronic communications services which are contrary to EU law, and which seriously interfere with fundamental rights of the persons whose data had been retained.

The CJEU unequivocally dismissed this possibility and clarified that only the CJEU may allow the temporary suspension of a rule of EU law with respect to national law that is contrary thereto. This is about primacy and uniform application of EU law – which would be undermined, if national courts were to give provisions of national law primacy over EU law, even only temporarily.[167]

As regards the question of what this means for criminal proceedings in which information and evidence obtained by a retention of data contrary to EU law was or is being used, the CJEU held that it is, in principle, for national law alone to determine rules on the admissibility and evaluation of such obtained information and evidence.[168] In the absence of EU rules on that matter, it is, in accordance with the principle of procedural autonomy, for the national legal order of each Member State to establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law.[169] However, Member States are not entirely free in doing so, as they need to ensure that these national rules comply with the principle of equivalence and the principle of effectiveness, i.e. that they are not less favourable than rules governing similar domestic situations and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law.[170] It is for the competent national court in criminal proceedings to ensure that these principles are safeguarded. However, the CJEU pointed out that it does not follow from the principle of effectiveness that unlawfully obtained information and evidence used in proceedings against a person suspected of the commission of criminal offences needs to be prohibited as such. For, other means may, too, serve the purpose of not prejudicing that person unduly by using unlawfully obtained material, such as national rules and practices governing the assessment and weighting of such information and evidence or the consideration whether such material is determining the sentence.[171]

The CJEU stressed that in deciding whether to exclude such information and evidence the competent national court needs to give particular attention to the adversarial principle, hence the right to a fair trial.[172] Accordingly, the right to a fair trial would be infringed, where the competent national court finds in a case that a party is not in a position to comment effectively on evidence which pertains to a field of which the judges have no knowledge and which is likely to have a preponderant influence on the findings of fact.[173] The national court must in such case disregard such evidence that was obtained by way of a general and indiscriminate retention of traffic and location data found to be in violation of Art. 15(1) of the e-Privacy Directive read in light of Arts. 7, 8 and 11 and Art. 52(1) of the Charter.[174]

The CJEU cited to that effect its jurisprudence in *Steffensen*,[175] which in turn refers to the decision of the ECtHR in *Mantovanelli v France*.[176] Both cases concerned technical issues before administrative courts, the former with regard to food safety, the latter with regard to liability in a case of medical maltreatment. The question arose as to whether the admission as evidence of results of expert analyses/reports on technical issues (quality of veal and pork sausages and respectively the excessive use of the anaesthetic Halothane), which went beyond the technical knowledge of the national court, entailed a risk of an infringement of the adversarial principle, given that in the *Steffensen* case the party was not given a right to request a second opinion in violation of EU law[177], while in *Mantovanelli* the party was entirely excluded from the preparation of the expert report.[178] Thus, although the administrative courts were not legally bound by the expert's findings, the technical analysis/report was likely to have a preponderant influence on the assessment of the facts by the courts.

The cited cases concern the situation in which the admission of evidence before a national court must be assessed against the right to a fair trial as laid down in Art. 6(1) ECHR, hence in principle similar to the one in the case at hand. Given the very specific technical questions involved in the cited cases and in particular the difference in the procedures involved (administrative/criminal), with the specificities and safeguards necessary in the context of criminal proceedings, it is doubtful, however, whether the elaborations by the CJEU best capture and address the questions surrounding the use of unlawfully retained and/or accessed traffic and location data as evidence in criminal proceedings.

To that end, the ECtHR developed rich jurisprudence on Art. 6 ECHR. Generally, the ECtHR held that Art. 6 ECHR does not lay down any rules on the admissibility of evidence as such, which is primarily a matter for regulation under national law.[179] It hence cannot determine whether particular types of evidence, such as evidence obtained unlawfully, may be admissible. The ECtHR stressed, however, that the

proceedings as a whole, including the way in which the evidence was obtained, need to be fair.[180] It thereby looks at various aspects, such as the nature of the violation, whether the rights of the defence have been respected, the quality of the evidence, as well as the circumstances in which it was obtained and whether these circumstances raise doubt on reliability or accuracy of evidence, whether the evidence in question was or was not decisive for the outcome of the criminal proceedings, etc.[181] This test has been particularly also applied in cases concerning the question whether the use of information, which allegedly was obtained in violation of Art. 8 ECHR (right to respect for private and family life) as evidence rendered a trial as a whole unfair within the meaning of Art. 6 ECHR.[182]

In conclusion, it can be said that although national provisions on the admissibility and evaluation of unlawfully obtained information and evidence might differ across the EU, the jurisprudence of the CJEU and in particular also of the ECtHR on Art. 6 ECHR provides valuable guidance for national courts. Notwithstanding, it appears that a potential unlawfulness of a retention of or access to data used as evidence in criminal proceedings alone will hardly lead to an exclusion of that evidence from the criminal proceedings.[183]

IV. Considerations and Practical Implications for Data Retention Resulting from the Recent Jurisprudence

While it can be said that the CJEU in its recent judgements opened the door for a variety of possible exceptions to its established rule that a general and indiscriminate retention of traffic and location data is precluded, a legitimate question remains whether there is an actual possibility to walk through that door. While the openness from the CJEU might certainly be appreciated from the law enforcement perspective, if not so much from a privacy perspective, there are many practical, legal and technical aspects which need to be considered when trying to find solutions that can be applied in real life.

1. Safeguarding national security

To start with the most serious aim of safeguarding national security, the CJEU, as outlined above, allows for the preventive general and indiscriminate retention of traffic and location data. The criteria established in *Quadrature du Net* leave open a variety of questions. The CJEU requires to that end a serious threat to national security that proves to be genuine and present or foreseeable. All these requirements need to be defined in national law and the measure needs to be subject to judicial review.

Member States regularly establish a general risk assessment regarding their national security situation. While the retention, according to the CJEU, cannot be systematic in nature, the threat to national security, in effect and reality, could be of such nature. To defend their national interests and taking into account Art. 4(2) TEU, Member States may see the need to establish a consistently enduring high threat to their national security, which would justify the need for a generalised data retention scheme. It is likely that Member States and their national services are not going to have great difficulties to provide enough indications and evidence to establish such continuous state of being under serious threat. This is also comprehensible, as Member States would want to be on the safe side and rather assess a risk as too high than as too low, with the then devastating consequences. Such a scheme would enable national security services to make use of the retained data in their effort to more effectively prevent and combat threats to national security, in particular terrorist attacks. The notion of a serious threat, which is "genuine and present or foreseeable" seems to offer sufficient leeway for Member States to establish their own assessment and to retain data on that basis.

What further supports this view is that the CJEU presumes that the existence of a threat to national security in itself establishes a connection between the data to be retained and the objective pursued – a requirement that the CJEU established in its earlier jurisprudence and considered indispensable. The CJEU, however, fails to provide any reasons for why such connection "must […] be considered", as it states in its judgement.[184] This means essentially that, in the CJEU's view, terrorist activities endangering or affecting the entire population form in themselves an objective criterion establishing a connection, between the data of the entire population and the objective of combating certain activities, such as terrorist crimes. This seems to be a too far-reaching assumption.

Moreover, there is a certain ambiguity left with regard to the term "safeguarding national security", which the CJEU sees as protecting essential functions of the State and the fundamental interests of society.[185] Although not congruent, the understanding of the term "fundamental State interests" under Article L. 811-3 of the French *Code de la sécurité intérieure*, subject of review by the CJEU in *Quadrature du Net*, is rather wide and includes apart from the prevention of terrorism, the protection and promotion of major foreign policy interests, economic, industrial and scientific interests or the prevention of organised crime. These and similar interests, such as the national employment situation or the national social and health systems, could well become the guiding principles in defining national security. It would not be the first time that restrictive or protectionist measures are justified with national security reasons. Against the background

that according to the CJEU safeguarding national security encompasses the prevention and punishment of "activities capable of seriously destabilising the fundamental constitutional, political economic or social structures of a country", for which terrorist activities are mentioned by way of an example only, the scope of the data retention measure could in practice be interpreted a lot wider and used more frequently than initially envisaged or desired.

A key aspect for consideration by the Member States concerns the definition of a time limit and the possibility for a renewal of the instruction to the providers. How does this interact with the situation where there is a consistently high security threat in a Member State? Should national authorities in such situation request a fictitious shorter time period to comply with the CJEU's requirements and at the same time submit an advance request for renewal in order to avoid gaps in the retention, which would not only pose security but also legal risks?

Similarly, which competent national authority should request the instruction for renewal and which, if any, legal remedies are available to oppose such an instruction (and by whom – given that this measure would apply to everyone)? This might be left to the conditions and safeguards that need to be put in place, but the lack of clarity on these points and the level of uncertainty this leaves behind constitute serious challenges for all stakeholders involved.

Of crucial importance is the requirement that a court or an independent administrative body needs to verify that one of the situations justifying the general and indiscriminate retention actually exists and that the conditions and safeguards are observed.[186] Although this may reasonably be understood as a *prior* judicial review, the CJEU does not explicitly state so. Whether and under which conditions such judicial review may be carried out *ex post* and whether the court or independent administrative body will indeed be in a position to make such judicial assessment or whether it needs to rely to a large extent on the security assessment carried out and expert knowledge – hence be reduced to "rubberstamping" the request – remains to be seen.

Lastly, although this is not entirely clear from the judgement of the CJEU in the case *Quadrature du Net*, it is assumed that the data retained for the purpose of safeguarding national security may be used for any potential subsequent proceedings in a criminal investigation and prosecution, in particular in the situation in which a terrorist offence for which the data was retained could not be prevented and was actually committed. While the purpose of gathering intelligence information is to safeguard national security, *i.e.* to carry out preventive measures, the CJEU specifically mentioned prevention and punishment of the activities that threaten national security.[187] Otherwise, from a purely practical angle, it would seem very unsatisfactory to be able to retain such data while not allowing the use of it in a subsequent criminal case before a national court. Linked to this question is, however, the scope of such retention in respect of crimes directly or indirectly linked to e.g. terrorist crimes, such as money laundering. The focus of this problem could shift towards the question on admissibility and evaluation of evidence in criminal proceedings. Solely preventing a terrorist attack from happening on the basis of retained data and not consequently letting justice do its job, cannot be considered sufficient.

Overall, the CJEU opens a broad avenue for a general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security. At the same time, it leaves open many questions that, as a whole, could seriously undermine the efforts made by the Member States to fulfil the requirements of the CJEU's jurisdiction, most notably the compliance with fundamental rights of the Charter.

2. Safeguarding public security (criminal offences)

In respect of the retention of traffic and location data for the purposes of combatting crime and safeguarding public security, the CJEU concluded that a general and indiscriminate, systematic and continuous data retention scheme is not justified, even for the fight against serious crime or prevention of serious threats to public security.[188] However, as outlined in the previous sections, the CJEU did allow for the "targeted retention" of traffic and location data, under certain requirements.

This follows the logic of the *Tele2* decision, and the CJEU elaborates in greater detail and provides additional examples in its recent judgments. Thus, the CJEU clarifies that a person subject of a targeted retention measure must generally have been identified beforehand as someone posing a threat to public or national security in a proceeding under national law.[189] This is a rather significant restriction, given that the purported aim and benefit of data retention is to actually identify such an individual from a large pool of persons on the basis of the data retained. This might also lead to difficulties because of another requirement set by the CJEU, i.e. the retention period. The CJEU requests retention periods that are limited in time and that data must be erased or anonymised at the lapse of the retention period. It is not far-fetched to believe that in many cases some, if not all relevant data, has been already erased by the time the targeted person has been identified and a request for retention made, leaving only the data retained from the immediate past available.

Moreover, the question remains on how to apply the restrictions with regard to "persons concerned" by a targeted retention in practice. As pointed out by the Belgian Constitutional Court in its reference, the difficulty lies in deciding whose data should be retained in a targeted manner, without being discriminatory. Such categorisation may also be incompatible with the presumption of innocence. In addition, it is also questionable whether a targeted retention of individuals is technically even possible since traffic data does not automatically allow for the categorization of individuals.[190] Such approach does also not offer solutions in relation to those with criminal intent, who can always find ways to circumvent chosen criteria, including by using prepaid cards for a short time, as well as first-time offenders that could not have been previously identified.[191] An additional challenge exists in cross-border situations, when persons concerned are frequently moving across borders, a tactic commonly used by organised crime groups, making a continuous targeting difficult if not impossible. It may also be that persons concerned are registered with several providers and for service providers it is not easy to know exactly which particular person is making use of their services at a particular point in time. Service providers generally have information available about subscribers and contracts for their own billing purposes but defining which individual is making use of which particular service is a time-consuming and costly activity, if at all possible in view of the current and upcoming technological challenges, including the switch from 4G to 5G. Also, the possibility to retain data kept under enhanced end-to-end encryption methods by Over-The-Top content (OTT) services could ultimately render data inaccessible to law enforcement authorities. The switch to 5G in combination with the enhanced use of encryption methods may thus make it very difficult for service providers to retain (traffic and location) data of "persons concerned" in the context of a targeted retention scheme.[192]

As regards determining the geographical criterion by the national authorities, the CJEU seems to have "hot-spot" places in mind, with a high incidence of serious crime or that are particularly vulnerable to the commission of serious crimes, such as infrastructure, airports, stations or tollbooth areas. Although the avenue to apply a targeted approach in relation to specified geographical areas has been previously pointed to by the CJEU in *Tele2*, the questions on the practical applicability of such criterion remain persistent.

The retention of data related to a specific geographical area could equally easily be considered discriminatory and/or disproportionate. It could in practice entail that an extensive amount of data is retained from persons living, working or passing by the mentioned highly frequented areas without having any link to the objective pursued by the retention. Moreover, since the CJEU extended the use of the targeted retention *a fortiori* also to safeguarding national security, the geographical areas could (or should?) easily be extended preventively to areas targeted by terrorist attacks, such as large public places or areas housing governmental or state buildings.

In addition, the geographical criterion may not be consistent with the way service providers operate and it remains to be seen whether they can find technical and financially feasible ways of restricting the retention of data to specific areas. This very much depends on the location of the cell towers of each service provider. Furthermore, the signals put out by mobile telephones do not automatically correlate with predefined geographical limits and location data is not automatically included in the data collected by the service providers.[193]

Another consideration relates to the fact that certain types of crime, such as cybercrime, by nature cannot be restricted to specific geographical areas – they take place everywhere and from everywhere. Cyberspace is by definition not bound to geographical locations. But a restriction on the basis of a geographical location may also not be feasible for the more "general crimes." For example, many forms of organised crime cannot be restricted to specific geographic areas as a change in location is often part of the criminal strategy of organised crime groups.

An additional complication in this context concerns the different legal regimes service providers have to comply with, especially when they are operating at the EU or global level. Even if technical possibilities may be explored and created to ensure the retention of data related to specific individuals or specific geographical areas, such solution is likely to be burdensome and costly. Investments already made by service providers for accommodating and maintaining data storage centres may not be sufficient for a targeted retention approach. Technical expertise to maintain and keep up to date these systems is needed[194] and service providers have to mitigate data breaches and cybersecurity risks. Reimbursement schemes by governments to cover for such costs vary greatly (and generally do not involve the investment costs that need to be made at the beginning) and it could therefore be the case that ultimately consumers will have to carry those costs themselves.

Furthermore, as regards the retention period, beyond the still unanswered question about the appropriate – or proportionate – length of such period, the CJEU allows the possibility for extensions, similarly to the case of safeguarding national security. All these extension decisions in themselves would impinge on the fundamental rights of the persons concerned. Nonetheless, unlike in the case of protecting national security, the CJEU does not explicitly mention any requirement for

a judicial review of such decisions here. These decisions are also separate from a request for access to such retained data, however, given their intrusive nature, effective judicial review seems indispensable in the context of the CJEU's approach of targeted retention.

Generally, the possibility of a targeted retention scheme is connected to the concept of serious crime. Art. 1(1) of the invalidated Directive 2006/24, which concerned the subject matter and scope, left the definition of "serious crime" to each Member States' national law.[195] While the CJEU established in *Tele2* that serious interferences can only be justified by the fight against serious crimes, it failed two years later to reply to the question of the referring *Tarragona* court in its decision *Ministerio Fiscal* what exactly determines the seriousness of the offence.[196] Although in its recent jurisprudence, the CJEU at least concedes that child pornography offences as defined in Art. 2(c) of Directive 2011/93[197] constitute serious offences,[198] it generally evades answering this question in full.

As the harmonisation of the definition of serious crime seems, as it currently stands, is not possible at the Union level, given the lack of harmonisation of substantive criminal law and the specificities of each national judicial system, an incoherent application of the concept of "serious crimes" inevitably leads to divergences in the interpretation and application of the CJEU's jurisprudence, as well as in the use of data retention rules across the Union and eventually in the level of protection of fundamental rights. Even if the list of serious crimes within Member States were to be identical, it could still lead to discrepancies between Member States and a potential unequal treatment of suspects and accused persons, in particular in cross-border situations.

It may also lead to unwelcome situations where certain crimes, which are considered to be minor, e.g. online fraud, are part of a bigger scheme of serious crimes, which could not have been uncovered without the retention of this data. Moreover, there are also crimes that may not be considered "serious", such as cyber-grooming or stalking, where the retained data remains the only information available to identify a suspect and bring the crime to justice.

In sum: same as in the case of safeguarding national security, the CJEU reinforces its jurisprudence in favour of a well-designed "targeted retention" of traffic and location data for the purpose of safeguarding public security, however, it leaves many questions open and does not sufficiently outline how such design could work in practice. Data retention for the purpose of fighting (serious) crimes remains therefore challenging for the Member States, bearing the risk of failing to comply with the CJEU's jurisdiction and fundamental rights of the Charter.

3. Retaining IP addresses and civil identity

Concerning the retention of IP addresses, the CJEU has taken into account considerations put forward by a number of Member States and acknowledges that, where an offence is committed online, the IP address may be the only means of investigation to identify the person to whom that address was assigned at the time the offence was committed.[199] This outcome resembles the findings of the Constitutional Court of Portugal in the case cited above (II.3). Nonetheless, for all the operational reasons that might speak in favour of the retention of IP addresses, the purpose driven approach followed by the CJEU is somehow unsatisfactory, given the significant impact of this exception.

Generally, the CJEU neither proffers convincing legal arguments for the conclusion reached, nor is the required connection between the data retained and the objective pursued, as required under the CJEU's case law, visible neither at first nor at second sight. It is also astonishing that the CJEU builds its argument around the circumstance that IP addresses would otherwise be unavailable as they are not retained by the providers of electronic communication services.[200] In fact, the non-retention results from the very fact that internet users enjoy the same protection of their fundamental rights under Arts. 7 and 8 of the Charter also in relation to IP addresses.

The CJEU also does not draw any distinction between static and dynamic IP addresses. While the desired goal – the identification of the user – is the same, the legal and practical handling of static and respectively dynamic IP addresses differ. From a technical point of view, dynamic IP addresses are more difficult to obtain for law enforcement authorities as more data is needed from service providers to identify the user behind a connection. Since identifying the users behind dynamic IP addresses generally requires the use of other data, it is hence unclear whether they fall under the CJEU's ruling related to the generalised retention possibility for IP addresses assigned to the source of a connection. Thus, the CJEU misses an opportunity to elaborate in greater detail on justifying this exception and the related questions, and whether this measure is indeed suitable and effective in pursuing the desired objective, i.e. to identify the end user.

Furthermore, the IP address itself may not be sufficient and other identification data needed to identify a relevant user in an investigation, for example the connection port, the date and time of the connection and its duration as well as the Media Access Control (MAC) address and the International Mobile Equipment Identity (IMEI) code. This information is often difficult to obtain when the Network Address Translation (NAT) technology is used. IP addresses, especially dynamic

IP addresses, are often assigned to more than one end-user because of the wide use of NAT technology. NAT is used to thwart the limited availability of IPv4-addresses to make connections. Using NAT, there could be thousands of users linked to one single public IP address, making it virtually impossible to identify the user who is of interest in a criminal investigation. And even if only a relatively small number of potential subscribers are identified as potentially relevant to the case, this will mean that investigative powers will have to be used against innocent citizens in order to identify the single user of interest. This infringement of fundamental rights could be mitigated or even avoided if the system was such that only the relevant subscriber could be identified. In addition, it is even more difficult to identify the relevant user when persons are using the internet or other digital services in public spaces such as internet cafés.

The issues linked to the NAT technology and dynamic IP addresses are not new. Although the more advanced IPv6, which makes available an immeasurable amount of IP addresses for use and thus makes the use of the NAT technology obsolete, became available in 1999, technical problems still persist. In fact, to date, the IPv4 and IPv6 systems exist in parallel.[201] According to the Google statistics consulted in September 2021 the availability of IPv6 connectivity in the EU ranges from 2% in Spain to 52% in Germany[202]. It can be expected that this situation is still going to remain at least in the short to medium term. For service providers it remains very complex and costly to retain the information necessary to identify users via dynamic IP addresses and they hence do not see the need to retain them except they are under legal obligation.

Another complication that should be kept in mind is that those with criminal intent could make use of modern software to anonymise and hide their IP addresses. In addition, the question also arises what is considered to be a reasonable time for retaining IP addresses.

As regards the data relating to the civil identity of users of electronic communications systems, the CJEU considers the retention of this data category to be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general and safeguarding public security, without imposing any limitations as regards the retention period. While the CJEU seems to try its best to offer more openings to the current difficulties for law enforcement authorities, the exact scope of this part of the ruling is not entirely clear. In particular, it is unclear whether the civil identity data category concerns the same type of data as the subscriber data category, in line with the definition used in the e-evidence package[203] and the Budapest Convention[204]. In order to better understand the practical implications of this concept, it would be useful to know from the CJEU which data can be retained in relation to the civil identity of a user. Moreover, given that even a non-serious interference with fundamental rights still remains an interference that needs to comply with the requirements of Art. 52(1) of the Charter, it would have been desirable, if the CJEU had elaborated in greater detail on the reasons which led to its conclusions, when it sought to strike a balance between the rights and interests at issue.

4. Expedited retention or "quick freeze"

As regards the possibilities of expedited retention, the CJEU acknowledges the situation that traffic and location data should be retained after the normal time periods for commercial processing and storage by the service providers have elapsed. This is the case where the data could be necessary to shed light on serious criminal offences or acts adversely affecting national security. The CJEU highlights that this could be in situations where the adverse effects on national security have already been established and where, after an objective examination of all circumstances, the adverse effects may reasonably be suspected.[205] The CJEU mentions that this measure can only be applied with regard to traffic and location data, that the duration must be limited to what is strictly necessary (with an extension possible), and that the instruction decision vis-à-vis the service providers should be subject to effective judicial review.[206] An extension of the retention possibilities to other persons is allowed, provided this is done on the basis of objective and non-discriminatory factors. Separate conditions are set out for the access to the data that was retained in this context.

In the absence of broader possibilities to retain data, the preservation of data related to a specific offence or a specific suspect was discussed as an alternative solution for law enforcement authorities. In Member States, this measure is usually referred to as the "quick freeze". If one can assume that the CJEU refers to the same notion, this measure refers to the request from law enforcement authorities or the prosecution service to preserve specific existing or past data stored by service providers for other purposes. However, as underlined by several law enforcement authorities, expedited retention is not really a suitable alternative to a generalised data retention scheme.[207] "Quick-freeze" merely saves available data from being erased, while the retrograde data that law enforcement authorities are most interested in cannot be retrieved *ex post.*[208] Moreover, the mechanism of a quick freeze can only apply from the moment there is a suspicion of a crime. This makes it necessary that at least a level of suspicion is established and a specific person is identified as suspect and at that point in time, there is still relevant data to be frozen. Furthermore, the success of the

measure very much depends on the national legal framework in place and if, and what types of data are (mandatorily or voluntarily) kept for which time period by service providers. Even if the national legislation allows for the preventive and mandatory retention of data by service providers in order to later on be able to request for a quick freeze, the reality is that, in comparison to a generalised data retention scheme, not all types of data can be kept in the same manner and for the same period of time.[209] Again, the same question of what duration could be defined as strictly necessary leaves room for interpretation as well as the question at what point in time an extension of the measure should be requested.

Another practical difficulty for law enforcement and judicial authorities that may arise relates to the fact that access to preserved data obtained for the purpose of tackling serious crime or protecting national security is not allowed for prosecuting or punishing "an ordinary criminal offence". A similar discussion could be held here as was done regarding the notion of "serious crime" (see above 2.). What should be understood under these concepts, is left to Member States, hence the interpretation and application may vary. But what happens if an ordinary criminal offence is inextricably linked to the serious crime or national security situation for which access to the data was granted? Does this imply that the offences need to be investigated and/or prosecuted separately? Or, could this situation be left to be reconciled through national rules on the admissibility and evaluation of evidence?

Moreover, the CJEU widens the scope of this measure by stating that the data requested through a "quick freeze" need not be limited to the persons specifically suspected of the crimes or act in question but also to other persons or geographic areas. The question is how objective and non-discriminatory factors can be formulated in order to avoid that the data of random bystanders is retained, thereby seriously interfering with the privacy of a potentially large group of people. After all, it is relatively easy to argue that any data can "shed a light" – as the CJEU puts it – on offences or acts authorities became aware of. Furthermore, as previously mentioned, the exception of an expedited retention may be used in conjunction with other exceptions justified under Art. 15(1) of Directive 2002/58, which could lead to the situation that more data of a variety of persons is retained for different purposes and could be used in a combined manner.

5. Automated analysis and real-time collection

As regards the particularly invasive intelligence techniques of an automated analysis and real-time collection of traffic and location data, the CJEU, to a large extent, adopts the same requirements established in the context of measures for the purpose of safeguarding national security. Accordingly, all the points raised under III.2.c) aa) above are valid here too. This concerns in particular the scope of the term "national security", the possibility for an enduring threat, the assumption (or rather the absence) of the existence of a link between all those whose data will be analysed (i.e. all persons using electronic communication systems!) and the threat, the scope and effectiveness of judicial review, and the handling of linked offences identified. Also, the terms and conditions applied by the CJEU – "valid reason to suspect" an involvement "in one way or another in terrorist activities" – seem to offer wide room for interpretation despite the very intrusive quality of the measure in question.

Moreover, given the specific nature of this measure, which applies parameters based on pre-established models and criteria, additional questions arise. The CJEU clarified that these models and criteria have to be determined in a non-discriminatory manner. But in a similar way as in the case of "targeted retention" (above III.2.c) bb)), this requirement imposed by the CJEU might turn out to be difficult to apply in practice. The use of pre-defined and set parameters might lead to a lack of traceability and comprehension of the output. For this reason, it might also be difficult to define the subject of judicial review. Moreover, such systems often bear the risk of generating a (at times significant[210]) number of wrong hits and errors and generally have an inherent deficiency with respect to transparency and control. It is doubtful that a manual review alone would be able to address such errors and deficiencies. In addition, a manual review of an automatic decision-taking system may also bear the risk of merely legitimising the automated decisions taken, without actually making the necessary comprehensive assessment due to the potential volume and the time constraints.[211] In the end, it remains entirely unclear, who should control and review such systems that are run by private service providers, on which basis and how often.

V. Data retention in the context of the negotiations on the e-Privacy Regulation

On 10 January 2017, the Commission put forward a proposal for a e-Privacy Regulation[212] to update the current rules to technical developments, to adapt them to the GDPR and to repeal the "e-Privacy Directive" from 2002. The objective of the e-Privacy Regulation, which, unlike the Directive, would apply directly across the Union, is to reinforce trust and security in the Digital Single Market, in particular strengthening security and confidentiality of communications and establishing clearer rules on tracking technologies, including cookies as well as on spam.[213] The e-Privacy Directive was considered not to keep pace with the technical developments leaving a

void of protection of communications conveyed through new services. The Commission proposal did not explicitly make any specific provision on data retention. It merely echoed in its Art. 11 the substance of Art. 15 of the current e-Privacy Directive. However, the draft Regulation aligns the scope of Art. 11 with Art. 23(1) GDPR, thus in effect, widens it considerably by introducing a general clause of "other important objectives of general public interest of the Union or of a Member State" to the list of objectives for which the rights enshrined in the draft Regulation may be restricted. Member States may hence keep or create national data retention regimes that provide, *inter alia*, for targeted retention measures, in so far as such regimes comply with Union law, taking account of the CJEU's jurisprudence on the interpretation of the e-Privacy Directive and the Charter.[214]

The European Parliament (EP) adopted its report on the draft proposal in the same year.[215] With regard to Art. 11 of the draft Regulation, the EP seeks to strengthen the safeguards, notification and transparency requirements as envisaged in the GDPR; however, the EP supports a narrower and more precise list of objectives provided in Art. 11 of the proposed Regulation, which may justify a restriction of the rights. It hence supports deletion of the general clause of "other important objectives" from that list.

The Council took more than four years to adopt its negotiation mandate under the Portuguese Council Presidency on 10 February 2021.[216] The question on data retention has been a highly debated issue discussed during the negotiations in the Council, in particular following the latest judgements of the CJEU.[217] Art. 2(2) of the General Approach of the Council provides for the material scope of the Regulation and stipulates that it shall not apply to

> (a) activities falling outside of the scope of Union law and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities, whether it is a public authority or a private operator acting at the request of a public authority.

According to the Council's General Approach, the Regulation's material scope shall also not apply to

> (b) activities, including data processing activities, of competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

In particular, the exclusion of retaining data for national security purposes from the scope of the proposed Regulation, as listed in Art. 2(2)(a) of the Council's General Approach, seems to be a response to the case law of the CJEU in relation to Arts. 1(3) and 15(1) of the e-Privacy Directive. This echoes the findings of the CJEU in the recent cases, where the CJEU differentiated between the old and repealed data protection Directive 95/46 and the e-Privacy Directive (see details above under III.2.a). Following its General Approach, the Council text would swipe away the jurisprudence of the CJEU at least as far as it concerns national security and defense. This would also, in a way, reinstate the situation as under Directive 95/46, which was overcome by the GDPR. In consequence and as intended, measures such as the retention of data in the context of safeguarding national security and defense would fall within the sole responsibility of national law and the ECHR. Nonetheless, given the role of the CJEU as the guardian of the Charter, it could be that the CJEU would review the principles it had established with regard to the protection of the fundamental rights under Arts. 7, 8 and 11 of the Charter directly, given the CJEU's broad understanding of "implementing Union law" within the meaning of Art. 51(1) of the Charter.[218] This means that even if the e-Privacy Regulation were to entirely exclude the retention of traffic and location data from its scope or for safeguarding national security and defense only, and instead this would be governed solely in national law, the CJEU could review the compliance of such national provisions with Arts. 7, 8 and 11 of the Charter in any case.

In respect of the fight against crime and the protection of public security, Art. 6(1)(d) of the Council text permits service providers to process electronic communications data where it is necessary to comply with Union or national rules to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security. Art. 7(4) of the Council text acts as the general rule on data retention and allows Union or national law to retain electronic communications metadata for a limited period of time in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security under the condition that the essence of the fundamental rights and freedoms is respected and it is a necessary and proportionate measure in a democratic society. In comparison with the jurisprudence of the CJEU, the Council's General Approach leaves out the distinction between the notions of serious crime and criminal offences in general as well as the conditions linked to the retention thereof. Moreover, the General Approach does not make any distinction for data categories.

The Council's General Approach received fierce criticism, for instance by the German data protection authority, which generally sees in it a "harsh blow to data protection", while expressing serious concerns with regard to the revisions made on data retention.[219] Finding a common ground on the e-Privacy Regulation has been challenging in the course of the last four

years. The trilogue negotiations started on 20 May 2021 and it is difficult to predict what the outcome of these negotiations will be. There is a clear need to update the 20-year-old e-Privacy Directive with a modernised piece of legislation. Going back in time to the level of Directive 95/46 for the purpose of excluding retention measures to safeguard national security from the scope of the new e-Privacy Regulation seems not to be a viable way. Moreover, as seen, the desired result – taking data retention for the purpose of safeguarding national security out from the scope of the proposed Regulation and the review by the CJEU – could in the end turn out to be wishful thinking. Despite all the misgivings expressed by the Parliament against and, by contrast, the strong wish expressed by the Council for a data retention regime, a set of recalibrated rules on data retention following the lines and limits set by the CJEU might be a prudent and yet feasible way forward for the e-Privacy Regulation after all.

VI. Conclusions

Data retention is not off the table. It never was. However, the discussions surpass the more radical (and at times emotionally charged) discussions *pro et contra* data retention as such and, thanks to the CJEU, now take a far more differentiated and diligent shape. The CJEU shed light on and recalibrated in detail the various facets of this wide, complex, and sensitive field of law, politics and life. It sought to establish a balance between the various entangled fundamental rights and freedoms. This debate that is often being portrayed as a "clash" between those who seek to defend liberty and those who seek more security will continue. And that's good. Each society and generation have its own expectations and faces its own challenges, while, with the changes that emerging (not least digital) technologies bring about, the questions surrounding the two notions of liberty and security remain to be asked and will need to be answered now as well as in the future. That is what the CJEU does in the EU's area of freedom, security and justice and this is what the CJEU needs to do.

The CJEU is also not legislating, as it is sometimes said. The CJEU, in the cases brought before it, sets the limits it sees as being necessary in order for legislation to comply with the principle of proportionality and the EU Charter of Fundamental Rights. That is what the legislator has to respect if it wishes to regulate the retention of data for the purpose of preventing serious threats to national security and combating crimes. The limits apply to both, the EU legislator in the event that this matter is regulated at EU level or, in the absence of EU action, the national legislator, who is bound by the principles and safeguards enshrined in the Treaties. Notwithstanding, data retention raises a number of questions.

From the outset, firstly, the legislator would need to proffer convincing evidence why it chooses to impose obligations on private providers of electronic communication services to retain different types of data in order to allow access to competent national authorities. Is the retention of data capable of bringing the desired added value in the prevention of serious threats to security and combating crimes? This question has been consistently flagged in the past, but has not been convincingly answered to date. It is a legitimate question, given the inherent serious interference with and violations of fundamental rights of a potentially very large number of persons (if not the entire European population), who might be entirely unrelated to the pursued objectives – something that could be depicted as a "mass incrimination".

The scarce number of studies that attempt to shed light on this question all struggle with the lack of reliable information. The very illustrative and extensive study prepared by the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, dates back to 2011 but still provides valuable insight and anecdotal evidence in this matter.[220] It particularly highlighted the lack of reliable statistical data and systematic empirical studies as well as the rather diverging views of the practitioners consulted.[221] Although the experience from anecdotal evidence provided in the study might be considered as exemplary, such evidence cannot be considered empirically deduced or proven. The Max Planck study outlined that, overall, there are no reliable indications that the retention of traffic and location data had an impact on the conviction rates. It particularly also did not find any indication that retained traffic or location data had any impact on the prevention of terrorist activities, while there are reasons to believe that such data might contribute to the investigations in the aftermath of terrorist acts. Against the background of the lack of relevant and/or reliable data, the study stressed that it is not excluded that traffic and location data could provide indications to initiate investigations and support complex investigations.[222] But even if such anecdotal evidence could indeed be established, such evidence alone would have no significant impact on the overall picture. However, for want of relevant and reliable data, it is difficult to use the study in favour or against data retention.

The study[223] prepared by the Legal Service of the European Parliament also deplores the lack of data and stressed particularly that it is not possible to establish a direct correlation between the existence of data retention laws and crime statistics. The study indicated that too many parameters need to be considered in order to be able to evaluate the reason for statistical changes.[224] The same problem is outlined in the most recent study on this matter, commissioned by the European Commission.[225] This study, which looked into the legal framework and

practices of ten Member States, yet highlighted that the information cannot be seen as representative of the stakeholders' view due to the limited information on this issue.[226]

The CJEU does not seem to question the added value of a data retention regime, when it stated in its decision *Digital Rights* that the eventually invalidated Data Retention Directive may be considered appropriate for attaining the objective pursued, without providing any reasons how it reaches such conclusion. Indeed, the question whether a measure is suitable or appropriate to attain the desired purpose may be posed several times when reading the recent judgements of the CJEU on data retention. When examining the measures, the CJEU seems to simply want to assume that this is the case – i.e. that the measure is indeed appropriate. This approach gives a blemish to the various exceptions justifying an interference with the fundamental rights of the European citizens, as put forward by the CJEU. But beyond that, from a more political point of view, the legitimacy of such invasive measures could be considerably increased, if the European and/or national legislator were to provide substantiated and convincing evidence of the added value of a data retention regime. This would also help in overcoming any polarising and simplistic debates on this important matter.

Secondly, in the decisions on data retention, the CJEU very much acts like a constitutional court. This is yet another *facette* of the CJEU, in addition to the broad variety of matters it has competence over (most recently, also in criminal proceedings of the European Public Prosecutor's Office[227]). The CJEU had to deal with the protection of fundamental rights in the past, prior the enactment of the Charter on Fundamental Rights. Already in 1969, the CJEU established in the *Stauder* case that fundamental rights are part of the general principles of Community law and that they are protected by the CJEU.[228] Nonetheless, thorough reflection should be spent on the question whether the existing structure of the CJEU and the legal and procedural framework is indeed best suited for the CJEU to carry out multiple functions as "one court for everything" and grant and ensure the necessary effective legal and judicial protection of fundamental rights in the EU.

Linked to the protection of fundamental rights, questions arise in respect of the lack of coherence between the jurisprudence of the Luxembourg court and the Strasbourg court. Although the CJEU reiterated in its recent decisions on data retention that pursuant to Art. 52(3) of the Charter, the corresponding rights of the ECHR form only the minimum threshold of protection, a divergent jurisprudence might lead to serious uncertainty with regard to the level of protection of human and fundamental rights in Europe, in particular also as the CJEU in its findings stresses that the fundamental rights in the Charter correspond to the rights under the ECHR. Such lack of coherence could potentially lead to situations, in which Member States face conflicting obligations to be followed under the principle of primacy of EU law on the one hand and obligations under the ECHR on the other. Although such concern might be considered theoretical only, the present lack of coherence could undermine the existing complex multi-layered relationship between the CJEU, the ECtHR and national constitutional courts. Moreover, while Art. 53 ECHR leaves room for a higher protection of human rights at national level, as long as the minimum standards guaranteed under the ECHR are complied with, a higher level of protection under national constitutional law might run into conflict with the principle of primacy of EU law, if various different national standards exceeding those guaranteed under the Charter were to be applied.[229]

Another aspect concerns the review of the fundamental rights by the CJEU. The CJEU identifies a number of fundamental rights in the Charter – Art. 7 (respect for private and family life), Art. 8 (protection of personal data), and Art. 11 (freedom of expression and information) – and balances these rights and interests against those which follow from Art. 3 (right to the integrity of the person), Art. 4 (prohibition of torture and inhumane or degrading treatment of punishment), and Art. 6 (right to liberty and security). Thereby, the CJEU did not reach a very deep level of examination. It is striking that the CJEU did not even consider the legitimate rights and interests of the private service providers as enshrined in Art. 16 (freedom to conduct a business) of the Charter. In view of the various possible obligations that may be imposed on the service providers in line with the jurisprudence of the CJEU, which has a considerable impact on business decisions, and which entails significant costs (investment and running costs) it is remarkable that the CJEU, as the guardian of the Charter, remains entirely silent on this point, irrespective of the fact that in some cases these costs may be (fully or partly) reimbursed. Art. 16 of the Charter might deserve attention also from another perspective, touching the question of legal standing, namely whether, how and to which extent private entities, such as private service and network providers, may in themselves invoke the violation of Arts. 7 and 8 of the Charter in the context of the retention of traffic and location data of their users or subscribers, *i.e.* third parties, or at least "trigger" an incidental review of violations of these fundamental rights of their users and subscribers. Although legal persons may invoke the rights enshrined in Arts. 7 and 8 of the Charter[230], the CJEU has reviewed the compliance of national data retention regimes with the Charter and potential violations of Arts. 7 and 8 of the Charter in relation to users and subscribers only and not the service and network providers, while Art. 16 of the Charter has never been a subject of discussion in that context. In general, it would be desirable if

the CJEU developed a more elaborate approach in reviewing potential interferences and violations of fundamental rights in the EU.

Thirdly, while the CJEU cracked the door open to various exceptions justifying the retention of traffic and location and other data, it remains unclear whether Member States, in practice, may indeed safely walk through that door. Even if the CJEU recalibrated its jurisprudence on data retention and is expected to continue doing so in the future,[231] there are still many questions left open, which, if unanswered, will continue to hinder the efforts made by the Member States to establish a balanced and Charter-compliant data retention regime. Moreover, experience from the past has demonstrated that the judgements of the CJEU did not always lead to the desired common understanding on how to design a meaningful and functioning data retention regime that complies with the *acquis* and the Charter, nor has the recent jurisprudence of the CJEU, as seen in the different approaches taken after the *Quadrature du Net* judgement by the referring courts.[232]

The CJEU could and should have taken the opportunity to shed more light on the various legal questions, with regard to the terms and requirements it established on data retention and should also have taken to a greater extent a careful look at the practical feasibility of the solutions it suggests. It may be that this is left for future judgements the CJEU is going to render. However, given the importance of the matter and the significance for the protection of fundamental rights in the Union on the one hand and maintaining security on the other, this seems like a missed opportunity.

In his Opinion[233] delivered on 18 November 2021 on the pending cases C-793/19 *SpaceNet* and C-794/19 *Telekom Deutschland*, case C-140/20 *Commissioner of the Garda Siochana and Others* and joined cases C-339/20 *VD* and C-397/20 *SR*, Advocate General (AG) *Campos Sánchez-Bordona* hints to some of the concerns raised in this article. These include the boundaries for the invocation of national security to allow a general and indiscriminate retention of traffic and location data,[234] potential uncertainties with regard to the scope of state security,[235] the difficulties in developing criteria for an effective and non-discriminatory targeted retention,[236] and the distinction between static and dynamic IP addresses and the impact of the Ipv6 protocol.[237] However, the AG does not elaborate in greater detail on them. Overall, he restates the line, which the CJEU has taken in its judgments in *Quadrature du Net* and *Prokuratuur,* and remains silent on the various pertinent question that follow from that jurisprudence.

The protection of personal data is without doubt one of the Union's success stories. The Union sets and promotes very high standards, and its data protection *acquis* has become a "gold standard" that is referred to as a model also for other countries in the world. At the same time, the Union is a "Union that Protects" and there are several measures to be put in place under the Union's Security Agenda. In its various judgements on data retention over the past years, the CJEU never entirely closed the door to the possibility of retaining data for the purpose of safeguarding national security and fighting serious crimes. All discussion on this topic is therefore guided by the importance of providing effective tools to fight crime, on the one hand, and the need to respect fundamental rights, in particular the rights to privacy, protection of personal data, non-discrimination and presumption of innocence, on the other hand.

Undoubtedly protecting private data is of utmost importance. However, the rights and interests following from the e-Privacy Directive and Arts. 7, 8 and 11 of the Charter do not mean that those rights and interests prevail over all other interests. Personal data is generated and used in all our daily lives. Nonetheless, the protection of personal data needs to be balanced in a sound and sober manner with other objectives and against the legitimate rights and interests of others; it obviously cannot trump all other rights and interests. The protection of data must also not become an impediment to the dynamic process of digital development. This applies equally to the positive aspects of new technologies as well as to their negative ones (use to commit crimes). Eventually, it is also about the question which price we want to pay to live in a free and secure society and how much criminality our society is capable of accepting for the benefit of safeguarding fundamental rights and freedoms.

The ongoing negotiations on the e-Privacy Regulation could tackle some of the open questions and address practical impediments, as long as this will be a step forward (and not backwards in the form of limiting the scope). However, it is not possible to predict the outcome and the speed of the negotiations yet.

In view of the persisting uncertainty on this topic and in view of the recent jurisprudence of the CJEU on data retention, it seems clear that there is a compelling need for finding a common ground. Such common ground could be established by way of a legislative approach at least on a set of definitions and basic notions at the Union level. This approach could provide the desired added value and the necessary legal certainty, also given the increasing number of cross-border investigations and prosecutions in the EU and the fact that service providers are established all over Europe (and the rest of the globe). Definitions on the categories of data should be aligned as much as possible with the existing *acquis* and future instruments, e.g. the future legislation on the EU-internal e-evidence pack-

age. A legislative approach at Union level could also include the newly established notion of civil identity data. Although more difficult, EU legislation could also include specific time limits under which data may be retained, depending on the sensitivity of the data in question and the purpose for which it is retained. From a fundamental rights point of view, it could also be useful to define in which situations a prior judicial authorisation is required and how to handle urgent cases. Another legislative aspect could concern a transparency mechanism which would provide an overview on the use and frequency of the measures across the Union. Even if on a small scale, such common legislative approach could put data retention on a more solid ground than the highly useful but more request-driven and hence piecemeal approach provided by the CJEU through its jurisprudence.

In conclusion, the recent jurisprudence of the CJEU does not bring about the necessary clarity to mark an end to the discussions as to whether data retention is a suitable tool that provides added value in the prevention and investigation of crimes and the protection of national security in the EU. For this it leaves too many questions open, in particular on how to implement the requirements of the CJEU jurisprudence in practice. At the same time, following years of controversy and numerous judicial decisions at national, Union, and European level, one can hardly speak of a beginning of data retention in the EU; nonetheless, the recent jurisprudence of the CJEU at least opens up many new avenues for consideration and reflection. These new avenues could be taken up and possibly channelled to a new legislative proposal with a limited scope at Union level.

Even so, without clear and convincing reasons supporting the suitability and added value of data retention for the purpose of preventing and fighting crimes and safeguarding national security, any legislative measures discussed will always be marred with a stain. But the CJEU will soon have another opportunity to shed more light on this matter.[238]

Adam Juszczak
Senior Researcher in Law

Elisa Sason
Justice and Home Affairs Counsellor, Permanent Representation of the Netherlands to the EU

* The views expressed in this article are solely those of the authors and are not an expression of the views of their employer or the institution they are affiliated with.

1 Cf. the broad support expressed by Ministers at the March 2021 Justice and Home Affairs Council for a functioning data retention regime. The Portuguese Presidency stressed on that occasion: "The retention of data is a crucial tool for our law enforcement authorities when carrying out investigations, and it is clear the current situation of uncertainty increases the risks to the security of our citizens. Today we reiterated our commitment to finding a common solution; one which allows our police and judicial authorities to carry out their work while fully ensuring the rights to privacy of our citizens." See: Informal video conference of justice ministers – Consilium (europa.eu).

2 E.g. Germany's former Minister of Justice, Sabine Leutheusser-Schnarrenberger, „Goodbye Vorratsdatenspeicherung", *Verfassungsblog*, 8 October 2020, <https://verfassungsblog.de/author/sabine-leutheusser-schnarrenberger/>, accessed 9 August 2021.

3 Charter of Fundamental Rights of the European Union (hereinafter "Charter"), *O.J.* C 326, 26.10.2012, 391.

4 Cf. e.g. decision of the Constitutional Court of Romania, Decision no. 1258 of 8 October 2009, Official Gazette no. 798 of 23 November 2009, or decision of the Bundesverfassungsgericht (Federal Constitutional Court of Germany) of 2 March 2010, 1 BvR 256/08, both decisions rendered before the CJEU took a stance on the matter in its judgement of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger a.o.* The jurisprudence of the CJEU was taken into account by subsequent decisions in several Member States, such as Austria, the Netherlands, Slovakia, and Slovenia.

5 Cf. ECtHR, 25 May 2021, *Big Brother Watch and Others v the United Kingdom* (applications nos. 58170/13, 62322/14 and 24960/15); ECtHR, 25 May 2021, *Centrum för rättvisa v Sweden* (application no 35252/08); ECtHR, 2 December 2008, *K.U. v Finland* (application no. 2872/02).

6 Conclusions of the European Council meeting of 10 and 11 December 2020, EUCO 22/20, point 26, <https://www.consilium.europa.eu/media/47296/1011-12-20-euco-conclusions-en.pdf>, accessed 9 August 2021.

7 Cf. the informal video conference of justice ministers – Consilium (europa.eu).

8 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *O.J.* L 105, 13.4.2006, 54–63.

9 Judgement of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger a.o.*

10 Ibid, para 49.

11 Ibid, para 57.

12 Ibid, para 60.

13 Ibid, para 63.

14 Ibid, para 66.

15 Ibid, para 68.

16 Such as in Austria, Belgium, Slovakia, and the Netherlands.

17 The purpose of the data retention directive was to combat serious crime, not all types of crime – cf. Art. 1(1) of Directive 2006/24, *op. cit.* (n. 8).

18 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter "e-Privacy Directive"), *O.J.* L 201, 31.7.2002, 37–47.
19 Judgement of 21 December 2016, Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB/Watson*, para 59.
20 Cf. n. 19.
21 Ibid, para 85.
22 Art. 15(1) of the e-Privacy Directive – headed "Application of certain provisions of Directive [95/46]" – reads as follows: "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."
23 CJEU, *Tele2/Watson, op. cit.* (n. 19), para 89.
24 Ibid, para 90.
25 In *Digital Rights*, the CJEU did not see a need to examine the validity of Directive 2006/24 in the light of Art. 11 of the Charter, given the violation of Arts. 7 and 8 of the Charter, cf. CJEU, *Digital Rights Ireland and Seitlinger a.o.*, *op. cit.* (n. 9), para 70.
26 CJEU, *Tele2 Sverige AB/Watson*, *op. cit.* (n. 19), para 94.
27 Ibid, para 98, 99.
28 Ibid, para 100.
29 Ibid, para 102.
30 Otherwise, as the Court stressed, the national legislation in question would affect the essence of those fundamental rights, ibid, para 101.
31 Ibid, para 101.
32 Ibid, para 107.
33 Ibid, para 104, 105.
34 Ibid, para 108–111.
35 Ibid, para 115.
36 Ibid.
37 Ibid, para 116.
38 Ibid, para 117.
39 Ibid.
40 Ibid, para 119.
41 Ibid, para 120, 123.
42 Ibid, para 121.
43 Ibid, para 122.
44 Ibid, para 65–81.
45 Ibid.
46 Ibid, para 72, 73.
47 Ibid.
48 Ibid, para 75–78. Cf. also Advocate General Saugmandsgaard Øe's opinion of 3 May 2018 in the Case C-207/16 *Ministerio Fiscal*, para 47, where he makes a difference between data processed directly in the context of state activity of a sovereign nature and data processed as an activity of a commercial nature and made available to authorities subsequently.
49 Judgement of the Constitutional Court of Portugal of 13 July 2017, no. 420/2017. The judgement concerned a case of child abuse, where a request by a prosecutor for authorisation to transmit data to identify a user to whom an IP address had been assigned was rejected by the District Court of Lisbon in October 2016 on the grounds that the Portuguese Law 32/2008, which transposed Directive 2006/24/EC, was unconstitutional in view of the CJEU's *Digital Rights* decision. The Constitutional Court concluded that Portugal, when transposing the Data Retention Directive, introduced an extensive and complex framework, including on access to and protection of retained data, and that these differences ought to be taken into account. The Constitutional Court hence declared the retention of subscriber information with respect to dynamic IP addresses on the basis of the Portuguese Law as constitutional.
50 Constitutional Court of Belgium, Arrêt n° 96/2018 of 19 July 2018, A.10.4 : « Le Conseil des ministres insiste encore sur le fait que la Cour [Constitutionelle] a conclu au caractère disproportionné de l'atteinte au droit au respect de la vie privée par la loi du 30 juillet 2013 en raison de la combinaison de quatre éléments : le fait que la conservation des données concernait toutes les personnes, l'absence de différence de traitement en fonction des catégories de données conservées et de leur utilité, l'absence ou l'insuffisance de règles, ce qui constituerait une ingérence dans le droit à la protection de la vie privée. Or, ni la Cour de justice de l'Union européenne ni la Cour n'ont jugé que l'un de ces quatre éléments pouvait suffire à conclure au caractère disproportionné de la mesure. Le contrôle du principe de proportionnalité suppose en effet une approche globale. »
51 Cf. CJEU, *Tele2 Sverige AB/Watson, op. cit.* (n. 19), para 16.
52 Reference for a preliminary ruling from the Investigatory Powers Tribunal – London (United Kingdom) made on 31 October 2017 – *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (Case C-623/17), *O.J.* C 22, 22 January 2018, 29.
53 Request for a preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018 – *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées* (Case C-511/18) and request for a preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018, *French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs v Premier ministre, Garde des Sceaux, Ministre de la Justice* (Case C-512/18).
54 Request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 2 August 2018 – *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres* (Case C-520/18).
55 Request for a preliminary ruling from the Supreme Court (Estonia) lodged on 29 November 2018 – *H.K. v Prokuratuur* (Case C-746/18).
56 Judgment of 6 October 2020, Case C-623/17, *Privacy International*, para 29.
57 Decrees (France) No 2015-1185, 2015-1211, 2015-1639 and 2016-67.
58 Law of 29 May 2016 amending, in particular, the loi du 13 juin 2005 relative aux communications électroniques, Moniteur belge of 20 June 2005, p. 28070; the code d'instruction criminelle and the loi du 30 novembre 1998 organique des services de renseignement et de sécurité, Moniteur belge of 18 December 1998, p. 40312. Cf. CJEU, 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *Quadrature du Net a.o.* , para 54.
59 Constitutional Court of Belgium, Arrêt n° 96/2018 of 19 July 2018, B.3. and B.4.1, also referring to Parl. Doc., Chamber, 2015–2016, DOC 54-1567/001, p. 6.
60 Constitutional Court of Belgium, Arrêt n° 96/2018 of 19 July 2018, B.4.2.
61 CJEU, *Privacy International*, *op. cit.* (n. 56), para 44 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 99.
62 CJEU, *Privacy International*, *op. cit.* (n. 56), para 43, 42 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 98, 97. See also above II.2.
63 Joined Cases C-511/18, C-512/18 and C-520/18 Quadrature du Net a.o., *op. cit.* (n. 58), para 99 and earlier judgments of 4 June 2013, Case C-300/11, *ZZ v Secretary of State for the Home Department*, para 38; of 20 March 2018, Case C-187/16, *Commission v Austria (State printing office),* para 75 and 76; and of 2 April 2020, Joined Cases C-715/17, C-718/17 and C-719/17, *Commission v Poland, Hungary and Czech Republic* (Temporary mechanism for the relocation of applicants for international protection), para 143 and 170.
64 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 99.
65 CJEU, *Privacy International*, *op. cit.* (n. 56), para 40, 41, thereby making reference to the definition provided in Art. 4(2) of Regulation 2018/679.
66 CJEU, 30 May 2006, Joined Cases C-317/04 and C-318/04, *Parliament v Council and Commission*, para 56–59. Please also see in the context of PNR the requests for preliminary rulings in the cases C-148/20, C-149/20 and C-150/20 (Lufthansa).
67 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, 31–50. This directive was repealed with effect of 25 May

2018 by Regulation 2016/679 (General Data Protection Regulation – GDPR).
68 CJEU, *Privacy International*, *op. cit.* (n. 56), para 46 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 101.
69 Ibid.
70 CJEU, *Privacy International*, *op. cit.* (n. 56), para 47 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 102.
71 CJEU, *Privacy International*, *op. cit.* (n. 56), para 48 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 103. See also to that effect Advocate General Saugmandsgaard Øe's opinion, *Ministerio Fiscal*, *op. cit.* (n. 48), para 47.
72 Opinion of Advocate General Campos Sánchez-Bordona delivered on 15 January 2020 in the Joined Cases C-511/18 and C-512/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net* (C-511/18), para 65–76.
73 CJEU, *Parliament v Council and Commission*, *op. cit.* (n. 66), para 58.
74 CJEU, *Privacy International*, *op. cit.* (n. 56), para 82 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 168.
75 Ibid.
76 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 109, 113.
77 Ibid, para 115–117.
78 Ibid, para 118.
79 Ibid, para 125.
80 Ibid, para 125.
81 Ibid, para 126.
82 Ibid, para 128.
83 Ibid.
84 Ibid, para 130, 131.
85 Ibid, para 132, 133.
86 CJEU, *Tele2 Sverige AB/Watson*, *op. cit.* (n. 19), para 119.
87 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 135.
88 CJEU, *Tele2 Sverige AB/Watson*, *op. cit.* (n. 19), para 119.
89 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 136.
90 Ibid, para 139.
91 Ibid, para 146.148.
92 Ibid, para 152.
93 Ibid.
94 Ibid, para 153.
95 Ibid, para 154.
96 Ibid, para 155.
97 Ibid.
98 Ibid.
99 Ibid, para 157 and CJEU, 2 October 2018, Case C-207/16, *Ministerio Fiscal*, para 40 and 59.
100 Ibid, para 140, 157 and CJEU, *Ministerio Fiscal*, *op. cit.* (n. 99), para 62.
101 *Op. cit.* (n. 99).
102 Ibid, para 49.
103 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 159, 131, 158.
104 Ibid, para 140, 157.
105 Ibid, para 159.
106 Ibid.
107 Art. 2 lit. (g) of the e-Privacy Directive states:'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof. Pursuant to Arts. 6 and 9 of that Directive data related to value added services may be processed to the extent and for the duration necessary for such services, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers may withdraw their consent at any time.
108 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 161.
109 Convention on Cybercrime of 23 November 2001 (European Treaty Series – No. 185).
110 Cf. Arts. 14 and 16 of the Convention on Cybercrime.
111 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 164.
112 Not necessarily national competent authorities, which hence might also apply to the European Public Prosecutor's Office.
113 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 163, 164.
114 The CJEU does not demand a prior review by a court or an independent administrative body.
115 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 164. Art. 16(2) of the Convention on Cybercrime also allows for a renewal of a preservation order and considers a period of time as long as necessary, up to a maximum of ninety days.
116 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 165.
117 Ibid, para 160.
118 Ibid, para 165.
119 See above under III.2.c) aa).
120 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 172.
121 Ibid, para 173.
122 Ibid, para 177.
123 Ibid, para 176–179.
124 Ibid, para 181.
125 Ibid, para 182.
126 Ibid. Cf. to that end also CJEU, Opinion 1/15 of 26 July 2017, *EU-Canada PNR Agreement*. This agreement stipulated in its Art. 26(2): "The Parties shall jointly review the implementation of this Agreement one year after its entry into force, at regular intervals thereafter, and additionally if requested by either Party and jointly decided."
127 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 183.
128 Ibid, para 184–185 and Article L. 851-4 of the French Code de la sécurité intérieure.
129 Ibid, para 187.
130 Ibid, 188.
131 Ibid, 189.
132 Ibid, para 66.
133 Ibid, para 38, 39, 66, 67.
134 Ibid.
135 Ibid.
136 Ibid, para 67.
137 Ibid, para 190.
138 Ibid.
139 Ibid, para 190.
140 Ibid, para 191.
141 Ibid, para 166.
142 Ibid.
143 Ibid.
144 CJEU, *Tele2 Sverige AB/Watson, op. cit.* (n. 19), para 120.
145 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 189 and CJEU, 2 March 2021, Case C-746/18, *H.K v Prokuratuur,* para 51 and 58, compared to the CJEU's judgement in *Tele2 Sverige AB/Watson*, *op. cit.* (n. 19), para 120.
146 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 176 and 189.
147 *Op. cit.* (n. 145).
148 H.K. was found guilty of the commission, within a period of around one year, of a number of thefts of goods of a value of 3 EUR to 40 EUR, thefts of cash of a value between 5.20 EUR and 2100 EUR, use of another person's bank card and acts of violence against persons, who were party to the court proceedings against her.
149 CJEU, *H.K v Prokuratuur, op. cit.* (n. 145), para 27–29.
150 Ibid, para 29
151 Ibid, para 30.
152 Ibid, para 31.
153 Ibid, para 32.
154 Ibid, para 33.
155 Ibid, para 35.
156 Ibid, para 35.
157 Ibid, para 46.
158 Ibid, para 47.
159 Ibid, para 48.
160 Ibid, para 49, 50.
161 Ibid, para 52.
162 Ibid, para 54 and the cited case law.
163 Ibid, para 55.
164 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 79 and 213.
165 Ibid.
166 Ibid.
167 Ibid, para 214–218. The CJEU stated that the national court may exceptionally maintain the effects of a measure despite a breach of procedural rules, where it is justified by overriding considerations to nullify a genuine and serious threat, such as the interruption of the electricity supply in the Member State concerned, cf. CJEU, 29 July 2019, Case C-411/17,

Inter-Environment Wallonie and Bond Beter Leefmilieu Vlaanderen. The CJEU, however, further stressed that this exception does not apply in the case at hand, as the legislation under review would continue to impose obligations on service providers which are contrary to EU law and which seriously interfere with fundamental rights (para 219).
168 Ibid, para 222.
169 Ibid, para 223.
170 Ibid, para 223 and case law cited.
171 Ibid, para 225.
172 Ibid, para 226.
173 Ibid, para 226 and the case law cited.
174 Ibid, para 228.
175 CJEU, 10 April 2003, Case C-276/01, *Joachim Steffensen*.
176 ECtHR, 18 March 1997, *Mantovelli v France*, Appl. No. 21497/93.
177 CJEU, *Steffensen*, *op. cit.* (n. 175), para 52.
178 ECtHR, *Mantovanelli v France, op. cit.* (n. 176), para 36.
179 ECtHR, 12 July 1988, *Schenk v Switzerland*, Appl. no. 10862/84, para 45–46; ECtHR [GC], 11 July 2017, *Moreira Ferreira v Portugal* (no. 2), Appl. no. 19867/12 , para 83; ECtHR, 1 March 2007, *Heglas v the Czech Republic*, Appl. no. 5935/02, para 84.
180 ECtHR, 27 October 2020, *Ayetullah Ay v Turkey*, Appl. nos. 29084/07 and 1191/08, para 123- 130.
181 ECtHR [GC], 1 June 2010, *Gäfgen v Germany*, Appl. no. 22978/05, para 164.
182 This concerns, for instance, cases related to the use of evidence obtained by unlawful secret surveillance (ECtHR cases *Bykov v Russia* [GC], para 69–83; *Khan v the United Kingdom*, para 34; *Dragojević v Croatia*, para 127–135; *Niţulescu v Romania*; *Dragoş Ioan Rusu v Romania*, para 47–50), and search and seizure operations (ECtHR cases *Khodorkovskiy and Lebedev v Russia*, para 699–705; *Prade v Germany*; *Tortladze v Georgia*, para 69, 72–76, concerning the search of the premises of an honorary consul; *Budak v Turkey*, para 68–73 and 84–86, concerning, in particular, the importance of examining the issues relating to the absence of attesting witnesses.
183 Cf. e.g. the decision by the German *Bundesgerichtshof* (Federal Court) concerning the use of retained data as evidence in criminal proceedings in the context of the retention law being declared as unconstitutional by the German *Bundesverfassungsgericht* (Federal Constitutional Court), BGH, 4. November 2010 – 4 StR 404/10.
184 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 137.
185 Ibid, para 135.
186 Ibid, para 139.
187 Ibid, para 135.
188 Ibid, para 142.
189 Ibid, para 149.
190 Conseil d'Etat (France), decision in cases Nos. 393099, 394922, 397844, 397851, 424717, 424718 of 21 April 2021, para 53.
191 Ibid, para 54.
192 See also Milieu, "Study on the retention of electronic communications non-content data for law enforcement purposes", Publications Office of the EU (europa.eu), September 2020 (published on 7 December 2020 [ISBN: 978-92-76-22841-7]), § 9.2.2, p. 113.
193 Conseil d'Etat (France), *op. cit.* (n. 190), para 53.
194 Center for Democracy & Technology: <https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf> accessed 9 August 2021.
195 Cf also CJEU, *Digital Rights Ireland and Seitlinger a.o.*, *op. cit.* (n. 9), para 60.
196 CJEU, *Ministerio Fiscal*, *op. cit.* (n. 99), para 56.
197 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *O.J.* L 335, 17.12.2011, 1.
198 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 154.
199 CJEU, *Privacy International*, *op. cit.* (n. 56), para 154, and above under III.2.c)cc).
200 Ibid, para 154.
201 See also the Milieu study, *op. cit.* (n. 192) , § 9.2.2, p. 113, § 5.2, p. 52.
202 To be found under <https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption> accessed 9 August 2021.
203 See for an overview of the data categories proposed in the e-evidence Regulation: <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345> accessed 9 August 2021.
204 Art.18 of the Convention on Cybercrime, *op. cit.* (n. 109).
205 CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 154, 161.
206 Ibid, para 163–164.
207 Cf. also the Milieu study, *op. cit.* (n. 192), section 7.5.
208 Cf. also Max-Planck-Institut für ausländisches und internationales Strafrecht, "Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten", July 2011, p. 227.
209 Milieu, *op. cit.* (n. 192), section 7.5.2.
210 According to a report by the Swiss journalist Timo Grossenbacher, two out of three persons are wrongly suspected by the software used by the Swiss Police, *SRF* <https://www.srf.ch/news/schweiz/predictive-policing-polizei-software-verdaechtigt-zwei-von-drei-personen-falsch> accessed 9 August 2021.
211 On related questions of handling algorithms in the work of the police and judicial authorities, cf. M. Simmler, S. Brunner and K. Schedler, "Smart Criminal Justice – Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege", 2020, University of St. Gallen, available at: <https://www.alexandria.unisg.ch/261666/> accessed 9 August 2021.
212 Proposal of 10 January 2017 for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.
213 See for more background: <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform> accessed 9 August 2021.
214 COM(2017) 10 final, *op. cit.* (n. 212), §1.3 "Consistency with other Union policies".
215 <https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html> accessed 9 August 2021.
216 See T. Wahl, "Council Agrees on Negotiating Mandate for E-Privacy Regulation – Data Retention Included", (2021) *eucrim*, 30; Council doc. 6087/21 of 10 February 2021.
217 Progress report of the German Presidency to the Council of the EU, ST 13106/20 of 23 November 2021.
218 Cf. CJEU, 7 May 2013, Case C-617/10, *Åkerberg Fransson*.
219 Cf. <https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/ePrivacy_Verordnung.html> accessed 9 August 2021.
220 Max-Planck-Institut für ausländisches und internationales Strafrecht, "Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten", July 2011.
221 Ibid, p. 218.
222 Ibid, p. 221.
223 Study of the Legal Service of the European Parliament – General data retention / effects on crime, 10 December 2019.
224 Ibid, p. 3.
225 Milieu Study, *op. cit.* (n. 192).
226 Ibid, p. 14–15. The limitations of the study are that the sample of replies is not statistically representative for all law enforcement authorities and electronic communications service provider(s) in the 10 Member States and data gaps exist due to the reluctance (or inability) of stakeholders to share information on data retention; furthermore, comparability of the data collected is limited, given the differences in national definitions and practices.
227 See e.g. Art. 42 on judicial review of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, *O.J.* L 283, 31.10.2017, 1.
228 CJEU, 12 November 1969, Case C-29/69, *Erich Stauder v Stadt Ulm*.
229 Similarly, E. Tuchtfeld, "Towards a European Court of Fundamental Rights, How the European Court of Justice Becomes a Last Instance of Fundamental Rights Adjudication in Europe", *Verfassungsblog*, 19. October 2020 <https://verfassungsblog.de/towards-a-european-court-of-fundamental-rights/> accessed 9 August 2021.

230 CJEU, 14 February 2008, Case C-450/06, *Varec,* para 48; CJEU, 9 November 2010, Joined Cases C-92/09 und C-93/09, *Schecke GbR and Eifert v Land Hessen,* para 53.
231 Cf. Request for a preliminary ruling from the Bundesverwaltungsgericht (Germany) lodged on 29 October 2019 – *Federal Republic of Germany v SpaceNet AG,* (Case C-793/19) and *Federal Republic of Germany v Telekom Deutschland GmbH* (Case C-794/19); request for a preliminary ruling from the Cour Cnstitutionnelle (Belgium) lodged on 31 October 2019 – *Ligue des droits humains v Conseil des ministers* (Case C-817/19); reference for a preliminary ruling from the Supreme Court (Ireland) made on 25 March 2020 – *G.D. v The Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Ressources, Attorney General* (Case C-140/20); request for a preliminary ruling from the Cour de cassation (France) lodged on 24 July 2020 – *VD* (C-339/20) and 20 August 2020 – *SR* (Case C-397/20).
232 Conseil d'Etat (France) Decision in cases Nos 393099, 394922, 397844, 397851, 424717, 424718 of 21 April 2021 and Constitutional Court (Belgium) case nr. 57/2021 of 22 April 2021.
233 Opinion of Advocate General *Campos Sánchez-Bordona*, 18 November 2021, Joined Cases C-793/19 *SpaceNet* and C-794/19 *Telekom Deutschland,* Case C-140/20 *Commissioner of the Garda Siochana and Others*, and Joined Cases C-339/20 *VD* and C-397/20 *SR*. It is of note that the latter joined cases concerned particularly the relation between specific Union legislation on insider dealing, market manipulation and market abuse and the e-Privacy Directive as far as access to traffic and location data is concerned.
234 Opinion in *SpaceNet, op. cit.* (n. 233), para 41.
235 Opinion in *VD* and *SR, op. cit.* (n. 233), para 85, 86.
236 Opinion in *SpaceNet, op. cit.* (n. 233), para 43–50.
237 Opinion in *SpaceNet, op. cit.* (n. 233), para 83.
238 Cf. the requests cited in n. 231.

A Reasoned Approach to Prohibiting the *Bis in Idem*

Between the Double and the Triple Identities

Pierpaolo Rossi-Maccanico*

The *ne bis in idem* protection in Art. 50 CFR restricts the ability of EU and national enforcement authorities to prosecute or punish the same defendant for the same criminal offence more than once. Under the Member States' legal traditions, the notion of "same offence" or *idem* requires a triple identity: of the offenders, the material facts, and the protected legal interests. A broader notion of idem that only requires a double identity is laid down in Art. 54 CISA, which entails the prohibition of double prosecution of the same offender for the same "material acts". The CJEU's case law is inconsistent: sometimes the Court requires double identity, thus giving effect to Art 54 CISA (as far as intra-state judicial cooperation is concerned), while requiring triple identity in other cases, in particular in the area of competition law. With the *Menci* judgment the CJEU aligned the interpretation of the notion "same offence" in Art. 50 CFR to "same acts" in Art. 54 CISA, and hence based it on the double identity test. The two pending cases C-117/20 *bpost* and C-151/20 *Nordzucker et al.*, both relating to the area of parallel competition proceedings, cast a new light on the interpretation of the idem concept. With two opinions rendered on 2 September 2021, AG *Bobek* proposed a unified triple identity test. He argued that the CJEU should reverse its jurisprudence based on double identity because it gives rise to legal uncertainty. The present article argues that the AG failed to suggest a viable solution to interpret the idem notion in accordance with ECtHR case law. It is suggested not to get rid of the broader standard of protection against double jeopardy in the EU when justified but to supplement the requirement of "same acts" with the familiar conditions for extracontractual liability, including the conduct, its effects, and casual link.

I. Background

In the EU, the application of the *ne bis in idem* principle protecting defendants from double criminal proceedings has never been more confusing. National judicial and administrative authorities competent to enforce criminal, competition, tax, or other offences are increasingly confronted with legal uncertainties as to whether it is legitimate for them to pursue penalty proceedings in parallel with each other, both domesticly and across borders, for the same acts or for acts that are partially congruent. As an established general principle of law, *ne bis in idem* restricts their ability to prosecute or punish the same offence more than once if it can be qualified as "criminal".[1] The aim of the principle is essentially procedural as it is to prohibit the repetition of criminal proceedings after a first acquittal or conviction. However, it also has repercussions on substantive criminal law as it may preclude duplicate punishments for the same acts, even if they qualify as multiple offences, when pursued in succession.

As far as the EU is concerned, the *ne bis in idem* principle is enshrined in Art. 50 of the Charter of Fundamental Rights (CFR),[2] proclaimed on 7 December 2000 in Nizza, and now attached to the Treaty of Lisbon. The *ne bis in idem* guarantee under the CFR has the purpose of bringing clarity to the right established in different forms in the various EU Member States as it is intended to cover cross-border situations.

Prior to the CFR, the *ne bis in idem* principle was included in Art. 4 of Protocol No 7 to the European Convention on Human Rights (ECHR), signed on 22 November 1984 by the Contracting States.[3] Art. 4 of Protocol No 7 to the ECHR only applies internally within the individual Contracting States but is nevertheless relevant for interpreting the *ne bis in idem* principle at the EU level, considering that Art. 52(3) CFR states:

> [i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.

The European Courts (i.e. the Court of Justice of the EU(CJEU) and the European Court of Human Rights (ECtHR)) have traditionally given similar interpretations of the principle, since they both agreed that it prohibits the undue cumulation of proceedings of the same kind, namely criminal, for the same offence.

Hence, the CJEU followed the ECtHR case law whenever the criminal nature of an offence had to be determined. As the ECtHR held in *Engel*,[4] this determination needs to consider not only the classification of the legal provision in domestic law *(nomen juris)* but also the punitive and deterrent nature and the degree of severity of the penalties that may be imposed under the law for the offence.

The judicial assimilation of administrative penalties into criminal ones irrespective of the legal classification has caused an array of concurring administrative and criminal penalties and of successive administrative and criminal proceedings against the same defendant for substantially the same misconduct; normatively, the offences could be qualified to constitute different offences, but materially they were the same. Hence, the question was whether such cases concerned an *idem*.

Moreover, in accordance with Art. 50 CFR, the *ne bis in idem* protection also applies between the jurisdictions of several Member States.[5] This corresponds to the EU law acquis as it resulted from Art. 54 of the Convention Implementing the Schengen Agreement (CISA),[6] Art. 7 of the Convention on the protection of the financial interests of the Communities,[7] and Art. 10 of the Convention on the fight against corruption.[8]

As regards the application of the principle within the same Member State (purely domestic situations), the guaranteed right in Art. 50 CFR has the same meaning and the same scope as the corresponding right in the ECHR as referred to by Art. 4 of Protocol No 7.

Whereas the principle is worded as an absolute right under the ECHR, Art. 50 CFR entails that it can be subject to exceptions covered by the horizontal clause in Art 52(1) CFR laying down the conditions for limitations on the exercise of the rights and freedoms recognised by the Charter. In other words, *ne bis in idem,* as guaranteed in Art. 50 CFR, entails that a person cannot be judged again for acts for which he or she was already finally acquitted or convicted, except if such acts do not constitute the same offence (*idem*) or if authorised by a law that maintains certain conditions.[9]

In the two judgments of 20 March 2018 in *Menci*[10] and *Garlsson*,[11] the CJEU specified the conditions the concerned national legislations must meet to cumulate administrative and criminal penalties in successive proceedings, and thus to limit the right not to be punished twice under Art. 50 CFR in accordance with Art. 52(1) CFR.

The *Menci* case concerned duplicate criminal proceedings preceded by administrative penalty proceedings (with a criminal nature) for the same non-payment of VAT; the CJEU notoriously held that, under the escape clause of Art. 52(1) CFR, a limitation of the *ne bis in idem* principle due to the second prosecution was justified

> for the purpose of achieving […] complementary aims relating, as the case may be, to different aspects of the same unlawful conduct at issue.[12]

The CJEU further concluded that the cumulative punishments met an objective of general interest, and that the national laws at issue providing for two distinct prosecutions contained rules ensuring that the duplicate administrative/criminal proceedings would only lead to cumulative punishments where strictly necessary and proportionate.[13] This followed an attentive review of the relevant national provisions, and, subject to the confirmation by the referring court, the CJEU concluded that the double penalty proceedings system applicable in Italy in that case could be considered proportionate and did not go beyond what was strictly necessary to sanction the same VAT non-payment.

However, the *Garlsson* case, which concerned a similar constellation of a cumulation of an administrative fine for market abuse following a criminal detention penalty for the same acts, gave rise to unjustified *ne bis in idem* because the CJEU noted that the previous conviction was taken into account only if it consisted in a prior criminal fine. The CJEU found that, under the legislation at issue, the mitigation of penalties under the national legislation at stake appeared

> solely to apply to the duplication of pecuniary penalties and not to the duplication of an administrative fine of a criminal nature and a term of imprisonment.

For this reason the Court concluded that the double proceedings were contrary to the principle of proportionality. The CJEU found that this legislation

> does not guarantee that the severity of all of the penalties imposed are limited to what is strictly necessary in relation to the seriousness of the offence concerned.[14]

Hence, the CJEU concluded in *Garlsson* that the legislation at issue did not fulfil the obligation for competent authorities, in the event that a second penalty was imposed, to ensure that

> the severity of the sum of all of the penalties imposed does not exceed the seriousness of the offence identified.[15]

Such discordant judgments give rise to uncertainty about when the limitations of the *ne bis in idem* protection in case of successive punitive proceedings brought separately are acceptable. The reason is that the CJEU acknowledges that cumulative penalties can in principle be applied for concurring offences in different proceedings. However, a violation of the double jeopardy prohibition can only be justified if the second proceedings serve complementary purposes and the concerned person's burden for defence is limited to the necessary minimum. This, in turn, is only possible if the two distinct proceedings show a sufficiently close connection, both in substance and in time – an antinomy that is difficult to attain in practice.

The uncertainty concerns the existence of concurring penalties and, therefore, the *idem* concept. More precisely, the question is notably whether the notion of "same offence" should correspond to "same criminally punishable conduct", which requires a triple identity: of the offender, the material facts (*idem factum*), and the protected legal interests (*idem crimen*), and not a double identity of the offender and the material acts. In that respect, both the ECtHR and the CJEU have developed diverging case laws on the notion of *idem*, which I will address in the following section.

II. The Equivocal Case Law of the ECtHR and the CJEU on the Idem Concept

As regards the interpretation of the *idem* concept, the ECtHR developed a vast jurisprudence on the duplication of administrative penalties of a criminal nature and proper criminal penalties. Considering the scope of the *ne bis in idem* guarantee in Protocol No 7 to the ECHR, these cases concerned the same national legal order. The traditional interpretation of *idem* was based on the triple identity test including the requirement of *idem crimen*. This entailed that the same conduct could legitimately produce a combination of separate administrative/criminal proceedings that, due to their distinct legal qualifications, are separate offences.[16]

A turning point was the ECtHR's Grand Chamber judgment in *Zolotukhin*.[17] The judges in Strasbourg had to deal with a duplication of penalty proceedings, including a first set of disciplinary proceedings, which were qualified as criminal under the *Engel* criteria, followed by a second set of proper criminal proceedings – all based on the same acts of indiscipline.[18] The ECtHR made the examination of the identity of the offences subject to a test of their essential elements rather than their legal qualifications. It concluded that the *idem crimen* approach should be abandoned to allow a broader application of the *ne bis in idem* protection and held that:[19]

> [the previous] approach which emphasises the legal characterisation of the two offences [was] too restrictive on the rights of the individual. [Therefore,] Article 4 of Protocol No 7 must be understood as prohibiting the prosecution or trial of a second 'offence' in so far as it arises from identical facts or facts which are substantially the same.

The ECtHR concluded[20] that from that moment onward the examination of the *idem* notion should thus

> focus on those facts which constitute a set of concrete factual circumstances involving the same defendant and inextricably linked together in time and space, the existence of which must be demonstrated in order to secure a conviction or institute criminal proceedings.

In the subsequent landmark judgment, *A and B v Norway*, the ECtHR partially reconsidered the broad interpretation of the *ne bis in idem* protection in *Zolotukhin*, since the principle does not permit derogations under the ECHR.[21] It allowed a duplication of proceedings whenever these were "combined in an integrated manner so as to form a coherent whole". The combination of administrative and criminal penalties in separate proceedings was held permissible under four conditions, including: (i) the complementary purposes pursued by both proceedings addressing different aspects of social misconduct; (ii) whether the duality of proceedings concerned is a foreseeable consequence, both in law and in practice, of the same impugned conduct; (iii) whether there is a coordination between the relevant sets of proceedings that have to be conducted in such a manner so as to avoid duplication in both the collection and assessment of the evidence; and (iv), the proportionality of the overall amount of the penalties imposed.[22]

If the conditions were fulfilled, the ECtHR considered that, in fact, no genuine second set of proceedings took place, so that there was no *bis in idem* even if separate penalty proceedings took place to sanction separate offences. The blending of the *idem* concept with the *bis* element contributed to the lawfulness of duplicate proceedings.[23]

In parallel, the CJEU had developed its own jurisprudence on the *idem* concept, most notably in competition matters, where the principle also found vast application in the EU. The CJEU interpreted the *idem* concept as requiring the triple identity including that of the legal interest protected. The *ne bis in idem* protection was therefore understood as only precluding the European Commission or a national competition authority (NCA) from finding an undertaking guilty a second time if the same authority had already sanctioned a conduct as anti-competitive with an unappealable final decision.[24] Therefore, where the Commission carries on the competition proceedings after national proceedings, two sanctions are not necessarily ruled out, while "a general requirement of natural justice" mandates that the previous punitive decision is taken into account in determining the successive sanction to be imposed.[25] Moreover, the *ne bis in idem* principle does not preclude the Union from imposing sanctions on a person for the same facts for which he/she has already been sentenced or tried outside the Union unless this is precluded by an international agreement.[26]

At the same time, with the establishment of the EU area of freedom, security and justice, the CJEU consistently ruled in relation to Art. 54 CISA that a person whose case has been finally disposed of in a Member State cannot be prosecuted again on the same acts in another Member State, whereas the fact that the same acts can be legally qualified as a separate crime is irrelevant.[27] Thus, according to the CJEU, Art. 54 CISA provides that the same or similar acts should not be prosecuted twice even if qualified differently under two national criminal provisions. This can be explained by the aim of Art. 54 CISA to avoid restrictions to the right to move freely within the single area of freedom, security, and justice, as a consequence of which duplication of (criminal) prosecutions for the same acts are prohibited to a greater extent.

In the leading case on the *idem* concept, the CJEU determined in *van Esbroeck* that the notion of "same acts" must be interpreted irrespective of their legal qualification.[28] Mr van Esbroeck was indicted in Belgium for having *exported* narcotics to Norway, although he served a sentence in Norway for having *imported* narcotics into that country. It was evident that the defendant was being tried again for the same material acts corresponding to the same cross-border crime of exporting/importing narcotics. The different legal qualifications of the same material act by the two legal orders (Belgium and Norway) were thus irrelevant. Should one accept the different qualifications of the same criminal conduct by the two concerned legal orders, this would systematically restrict free movement and unduly double criminal prosecutions:[29]

> Because there is no harmonisation of national criminal laws, a criterion based on the legal classification of the acts or on the protected legal interest might create as many barriers to freedom of movement within the Schengen territory as there are penal systems in the Contracting States. In those circumstances, the only relevant criterion for the application of Article 54 of the CISA is identity of the material acts, understood in the sense of the existence of a set of concrete circumstances which are inextricably linked together. […] [T]he definitive assessment in that regard belongs […] to the competent national courts which are charged with the task of determining whether the material acts at issue constitute a set of facts which are inextricably linked together in time, in space and by their subject-matter.

Eventually, the CJEU felt obliged to systematise its interpretation of the *idem* concept under Art. 50 CFR as it is under Art. 54 CISA and also to align it to the conceptualisation by the ECtHR. With the above-referred contemporaneous judgments in *Menci* and *Garlsson* – dealing with duplications of administrative penalty proceedings (with a criminal nature) and proper criminal proceedings for the same acts – the CJEU extended its broad interpretation of *idem* to cover situations of duplicative administrative/criminal proceedings in the same national legal order.

The *Menci* case dealt with the sole owner of a business who had failed to pay a VAT debt within the prescribed deadlines in Italy; he was subject to an administrative penalty in an administrative proceeding and was successively charged in criminal proceedings. There was little doubt that the proceedings were a duplication (so-called "twin track" system). The Italian court that conducted the criminal proceedings asked the CJEU to rule whether, in the circumstances at issue, the *ne bis in idem* protection could limit the criminal prosecution of the tax offence in so far as the defendant was already sanctioned for the same facts in the administrative proceedings. The CJEU acknowledged that the *ne bis in idem* precluded a Member State from successively imposing a tax penalty with a criminal nature and a criminal penalty for the same act of non-payment of VAT. The CJEU stated in regard of the interpretation of the *idem* concept:[30]

> According to the Court's case-law, the relevant criterion for the purposes of assessing the existence of the same offence is identity of the material facts, understood as the existence of a set of concrete circumstances which are inextricably linked together which resulted in the final acquittal or conviction of the person concerned […]. Therefore, Article 50 of the Charter prohibits the imposition, with respect to identical facts, of several criminal penalties as a result of different proceedings brought for those purposes.
>
> Moreover, the legal classification, under national law, of the facts and the legal interest protected are not relevant for the purposes of establishing the existence of the same offence, in so far as the scope of the protection conferred by Article 50 of the Charter cannot vary from one Member State to another.

Here, the CJEU provided that the notion of "same offence" under Art. 50 CFR should follow the same interpretation as "same acts" in Art. 54 CISA. This entails protection against the risks of double jeopardy for the same material conduct even if it constitutes more than one offence.

Although the *Menci* judgment seemed to be composed of different lines of the CJEU case law, it raises even more questions, e.g.: what did the CJEU intend by the identity of the material facts to be "understood as the existence of a set of concrete circumstances which are inextricably linked together which resulted in the final acquittal or conviction of the person concerned"?[31] And is this interpretation only required "in so far as the scope of the protection conferred by Article 50 of the Charter cannot vary from one Member State to another"?

III. A New Opportunity to Clarify the *Idem* Concept

Against this background, the two currently pending cases C-117/20 *bpost* and C-151/20 *Nordzucker et al.*, both of which relate to the area of concurring competition proceedings, will give the CJEU the opportunity to cast a new light on the interpretation of the *idem* concept. In his two opinions rendered on 2 September 2021, Advocate General (AG) *Bobek* proposed a unified test of *idem* under the triple identity. He argued that the CJEU should reverse its jurisprudence based on the double identity because it gives rise to legal uncertainty and the risk of immunity. The facts of the two cases cast doubts on the double identity interpretation of *idem* as deriving from *Menci*.

In *bpost*, the Belgian Postal Authority (BPA) imposed in 2011 a fine of €2.3 million on the universal postal services provider bpost for violating the non-discrimination obligation in the Belgian law governing the opening of the market for postal services. The violation consisted in the application of a selective pricing system that denied certain quantity rebates to some business customers (aggregators in the collection of mail). After a separate enquiry in 2012, the Belgian Competition Authority (BCA) imposed a fine of €37.4 million on bpost for abusing its dominant position in violation of Art. 102 TFEU, based on the same selective system of rebates but with the different aim of excluding aggregators from the postal services market. In calculating the fine, the BCA deducted the fine that the BPA had imposed from the fine it would normally have imposed. The first fine by the BPA was contested by bpost and eventually annulled by the Belgian court on the ground that the rebate system was not discriminatory. The acquittal became final as the BPA did not appeal the judgment. Bpost then contested the second fine by the BCA on the ground that the *ne bis in idem* protection had been violated since the antitrust fine was based on essentially the same conduct. In the ensuing national competition proceedings, in which the European Commission intervened to defend the threefold identity test for *idem*, the referring court asked the CJEU whether the *ne bis in idem* principle bars the second competition proceedings even if they are based on a different legal interest than the postal proceedings.

In *Nordzucker et al.*, the Austrian Supreme Court was seized of proceedings in which the Austrian Competition Authority (ACA) sought to determine that two German sugar producers, Nordzucker and Südzucker, had breached Art. 101 TFEU by organising a cross-border cartel affecting the German and Austrian sugar markets. In these cartel proceedings, the ACA also sought the imposition of a fine on Südzucker with respect to that infringement, although Südzucker was previously sanctioned by the German Competition Authority for that reason with a fine of €195.5 million. In this context, the referring Austrian court raised several preliminary ruling questions about the interpretation of the *ne bis in idem* principle, and most notably about the legal requirements for the condition of *idem* under EU law.

AG *Bobek* supported a narrower scope for the *ne bis in idem* protection than in *Menci* by suggesting that the concept of *idem* requires the triple identity of the offender, the relevant facts, and the protected legal interest. He posits that the aim of the *ne bis in idem* principle is to protect a defendant from a second set of proceedings. Hence, the conditions for its application must be defined *ex-ante* and must be predictable and cannot depend on which authority comes first in sanctioning the facts.

IV. A Reasoned Approach to *Idem*

The pending cases in *bpost* and *Nordzucker* (described above) present a unique opportunity for the CJEU to clarify the *idem* concept. AG *Bobek* is right in identifying the inconsistencies in the CJEU's case law on *idem* by comparing the judgment in *Menci* with the one in *Toshiba* (detailed more precisely below) but he fails to reconcile the two judgments. While the AG held that the two rulings are mutually exclusive, he overlooked that *Menci* refers to a specific notion of *idem*, which combines the material with the procedural dimensions of the *idem* concept as held in *van Esbroeck*.[32] Such an approach entails an appropriate standard of protection against double jeopardy in the EU's single area of justice that is based on the mutual recognition and equivalence of the national punitive proceedings of another Member State. This equivalence finds its basis in an autonomous interpretation of *idem* created by the CJEU and is independent from the national legal qualifications consisting in "a set of concrete circumstances which are inextricably linked together which resulted in the final acquittal or conviction of the person concerned".[33]

I agree that the pending cases in *bpost* and *Nordzucker et al.* must be assessed against the background of the CJEU's case law in *Toshiba*, which in my view should be understood as being compliant with *Menci* and *van Esbroeck*, and not con-

tradicting them. *Toshiba* forms the most recent case in the area of competition, in which the judges in Luxembourg confirmed the triple identity test for *idem*.[34] The *Toshiba* case dealt with a preliminary ruling reference by a Czech court on the application of the *ne bis in idem* principle in the context of parallel competition proceedings that were first conducted by the Commission and then by the Czech Competition Authority with respect to the same EU-wide cartel. The Czech Competition Authority fined certain undertakings accused of participating in an international cartel between 1988 and 2004 on the market for gas-insulated switchgear for violating national competition rules, although the Commission had previously sanctioned the same cartel participants for violating Art. 101 TFEU. After having informed the Czech Competition Authority of its enquiry concerning the activities of the cartel in the EU territory before May 2004, i.e. prior to the accession of the Czech Republic to the Union, the Commission adopted its fining decision in January 2007 finding that certain undertakings had taken part in a complex EU cartel between January 1988 and May 2004. In February 2007, the Czech Competition Authority decided to sanction the Czech side of the cartel again by applying Czech law. The Czech authorities established that this cartel had taken place from July 2001 to March 2004, i.e., before accession, and sanctioned it accordingly. Against this backdrop, the main preliminary question raised in *Toshiba* was whether, under EU law, the same cartel violating both Art. 101 TFEU and the applicable national provision could only be sanctioned by the European Commission, which had acted first.

The CJEU confirmed the possibility of concurring proceedings and penalties being applied by separate competent authorities, each acting within the different scope of its respective jurisdictions and laws – namely, EU and national competition laws – and each dealing with a different set of facts. The CJEU called to mind: [35]

> […] in competition law cases, […] the application of this principle is subject to the threefold condition that in the two cases the facts must be the same, the offender the same and the legal interest protected the same.

This statement in the *Toshiba* judgment, however, seemed an *obiter dictum* because the CJEU eventually held that "in any event, one of the conditions thus laid down, namely identity of the facts, [was] lacking" in that case.[36] In *Toshiba*, the CJEU limited itself to pointing out that there was no identity of facts to start with without addressing whether there was identity of the legal interests protected in the national as opposed to the Commission's proceedings.

In so doing, the CJEU, however, used a narrower and more specific concept of identity of facts that transcends the notion of same acts but rather comprises its territorial or market effects. This conclusion in *Toshiba* should be stressed if parallels are drawn to the interpretation of *idem* between, on the one hand, *Toshiba* and, on the other hand, the cases in *bpost* and in *Menci.* As analysed above, the interpretation of the notion of *idem* in *Menci* does not refer to all the material acts but only to those that have led to a preceding final criminal conviction or acquittal or may lead to such a conviction or acquittal.

Against this background, one should note that a criminal conviction or acquittal generally relates to acts that may give rise or are otherwise akin to extracontractual liability. In that respect, the concept of same acts can be understood as comprising the three elements of a conduct (a material act or omission), its effects, and the causal link between the conduct and the effects.

In other words, I am of the opinion that, for a reasoned concept of *idem*, inspiration should be drawn from the CJEU's case law that requires the existence of three cumulative elements for tortuous acts. Thus, besides the material conduct, the *idem* requirement should comprise the effects of the conduct as well as the geographic and temporal scopes in which the conduct takes place. Moreover, the appraisal of *idem* should include its procedural dimension, since a conduct and its effects can only be determined by certain competent authorities which are able to conclude whether certain circumstances are part of the same *idem* and should be considered together. All such elements (effects, causal link, existence of proceedings) stem from qualifications in law of the material acts and complete the definition of *idem*.

In my view the situation in the *bpost* case concerns a concurrence of separate penalty proceedings in the same Member State by independent authorities; each proceeding corresponds to a different *idem* which cannot be considered a duplication already tried before as intended by the ECtHR in *Zolotukhin*. In the same vein, the *bpost* scenario does not fit with the conditions that the ECtHR laid down in *A and B v Norway*, where the ECtHR allowed a duplication of proceedings "combined in an integrated manner so as to form a coherent whole". The reason is that there should not be any integration between proceedings that are independent.

The above conclusion follows the CJEU's *dictum* in *Menci:* [37]

> The legal classification, under national law, of the facts and the legal interest protected are not relevant for the purposes of establishing the existence of the same offence. [That only applies] in so far as the scope of the protection conferred by Article 50 of the Charter cannot vary from one Member State to another.

In that respect, I find that the *bpost* case is not a matter of twin administrative and criminal penalty proceedings for the same acts but of different proceedings regarding different subject matters, which would be tried separately under any legal sys-

tem of any Member State. The duplication of proceedings thus does not violate the *ne bis in idem* principle, as it does not concern the twin-track punitive system of one Member State only.

Similarly, with respect to *Nordzucker et al.*, the parallel penalty proceedings of the Austrian Competition Authority and the German Competition Authority were not subject of the same *idem*: the first proceedings could not have sanctioned the infringement that was later the subject matter of the second proceedings because the latter has a different territorial scope.[38] In that case, the second proceedings are not "inextricably linked together [with the first proceedings] which resulted in the final acquittal or conviction of the person concerned", as intended in *Menci* and in *van Esbroeck*.

Pierpaolo Rossi-Maccanico

Attorney at Law. LL.M. International Tax Program, NYU '02. Chargé de cours *EU Business Taxation* at the European Business Law LL.M. Programme, Faculté de Droit et Science Politique, Université Aix-Marseille

* The author was involved in the cases C-117/20 and C-151/20 as an agent for the European Commission. The opinions expressed in this article are personal in nature and are the sole responsibility of the author.

1 B. van Bockel, Ne Bis in Idem in EU Law, 2016.

2 Art. 50 CFR (Right not to be tried or punished twice in criminal proceedings for the same criminal offence): "No one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law."

3 Art. 4 of Protocol No 7 to the ECHR (Right not to be tried or punished twice):

"1. No one shall be liable to be tried or punished again in criminal proceedings under the jurisdiction of the same State for an offence for which he has already been finally acquitted or convicted in accordance with the law and penal procedure of that State.

2. The provisions of the preceding paragraph shall not prevent the reopening of the case in accordance with the law and penal procedure of the State concerned, if there is evidence of new or newly discovered facts, or if there has been a fundamental defect in the previous proceedings, which could affect the outcome of the case.

3. No derogation from this Article shall be made under Article 15 of the Convention."

4 ECtHR, 8 June 1976, *Engel and Others v Netherlands*, Appl. no. 5100/71 et al., para. 82.

5 Explanations relating to the Charter of Fundamental Rights on Article 50, *O.J.* C 303, 14.12.2007, 17.

6 Art. 54 of the Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany, and the French Republic on the gradual abolition of checks at their common borders, *O.J.* L 239, 22.9.2000, 19, 35: "A person whose trial has been finally disposed of in one Contracting Party may not be prosecuted in another Contracting Party for the same acts provided that, if a penalty has been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing Contracting Party".

7 Art. 7(1) of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the protection of the European Communities' financial interests, *O.J.* C 316, 27.11.1995, 49, 51*:* "Member States shall apply in their national criminal laws the 'ne bis in idem' rule, under which a person whose trial has been finally disposed of in a Member State may not be prosecuted in another Member State in respect of the same facts, provided that if a penalty was imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing State." The Convention was replaced by Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law, *O.J.* L 198, 28.7.2017, 29. The Directive mentions the *ne bis in idem* protection in its Recital 21: "Given the possibility of multiple jurisdictions for cross-border criminal offences falling under the scope of this Directive, the Member States should ensure that the principle of ne bis in idem is respected in full in the application of national law transposing this Directive."

8 Art. 10(1) of the Convention drawn up on the basis of Article K.3 (2) (c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, *O.J.* C 195, 25.6.1997, 2, 4.: "Member States shall apply, in their national criminal laws, the *ne bis in idem* rule, under which a person whose trial has been finally disposed of in a Member State may not be prosecuted in another Member State in respect of the same facts, provided that if a penalty was imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing State."

9 ECJ, 5 May 1966, Joined Cases 18/65 and 35/65, *Max Gutmann v Commission*, p. 119 (as to the finding that the principle prevents the Union from imposing two disciplinary measures for a single offence and from holding disciplinary proceedings more than once with regard to a single set of facts); CJEU, 20 March 2018, Case C-524/15, *Menci*, paras. 40–62 (as to the limitations to the *ne bis in idem* principle).

10 CJEU, *Menci*, *op. cit.* (n. 9).

11 CJEU, 20 March 2018, Case C537/16, *Garlsson Real Estate SA and Others v Commissione Nazionale per le Società e la Borsa (Consob).*

12 CJEU, *Menci*, *op. cit.* (n. 9), para. 44.

13 CJEU, *Menci*, *op. cit.* (n. 9), paras. 63 and 65. A derogation under Art. 52(1) of the Charter could be made if the national referring court ascertained that the second proceedings and/or penalties:

(i) pursued an objective of general interest which is such as to justify such a duplication of proceedings and penalties, making it necessary for those proceedings and penalties to pursue additional objectives;

(ii) contained rules ensuring coordination which limits to what is strictly necessary the additional disadvantage which results, for the persons concerned, from a duplication of proceedings, and

(iii) provided for rules making it possible to ensure that the severity of all of the penalties imposed is limited to what is strictly necessary in relation to the seriousness of the offence concerned.

14 CJEU, *Garlsson Real Estate*, *op. cit.* (n. 11), para. 60.

15 CJEU, *Garlsson Real Estate*, *op. cit.* (n. 11), para. 56.

16 ECtHR, 30 July 1998, *Oliveira v Switzerland,* Appl. no. 25711/94, paras. 25–29; ECtHR, 29 May 2001, *Franz Fischer v Austria,* Appl. no. 37950/97, para. 29.

17 ECtHR, 10 February 2009, *Sergey Zolotukhin v Russia*, Appl. no. 14939/03.

18 The *Zolotukhin* case concerned a military member who was verbally abusive towards his superiors during his interrogation conducted for disciplinary purposes. In the ensuing administrative disciplinary proceedings conducted against him, which the ECtHR likened to a criminal procedure, he was convicted of "minor disorderly acts". Several days later, a formal criminal case was opened in respect of, *inter alia*, the charge of "disorderly acts". That charge referred to the same conduct for which the applicant had been previously convicted. The applicant was acquitted in respect of that charge but found guilty on other accounts based on the same acts of indiscipline.

19 ECtHR, *Zolotukhin*, *op. cit.* (n. 17), paras. 81 and 82.
20 ECtHR, *Zolotukhin*, *op. cit.* (n. 17), para. 84.
21 ECtHR, 15 November 2016, *A and B v Norway*, Appl. nos. 24130/11 and 29758/11. The case also concerned cumulative tax penalty proceedings (qualifiable as criminal under the *Engel* criteria) and criminal proceedings for the same failure to declare income on their tax returns conducted (to some extent) in parallel. The ECtHR concluded that that situation did not amount to a breach of Art. 4 of Protocol No 7 to the ECHR stating that: "whilst different sanctions were imposed by two different authorities in different proceedings, there was nevertheless a sufficiently close connection between them, both in substance and in time, to consider them as forming part of an integral scheme of sanctions under Norwegian law for failure to provide information about certain income on a tax return, with the resulting deficiency in the tax assessment".
22 ECtHR, *A and B v Norway*, *op. cit.* (n. 21), paras. 132, 147, and 153.
23 ECtHR, *A and B v Norway*, *op. cit.* (n. 21), para. 111.
24 Judgment of the Court of First Instance of 20 April 1999 in Joined Cases T-305/ 94, T-306/ 94, T-307/ 94, T-313/94, T-314/ 94, T-315/ 94, T-316/ 94, T-318/ 94, T-325/94, T-328/94, T-329/94, and T-335/94, *Limburgse Vinyl Maatschappij NV and Others v Commission* ('PVC II'), paras. 86–97, as upheld on appeal (judgment of the ECJ of 15 October 2002, Joined Cases C-238/99 P, C-244/99 P, C-245/99 P, C-247/99 P, C-250–252/ 99 P, and C-254/99 P *Limburgse Vinyl Maatschappij NV and Others v Commission,* paras. 59–63).
25 ECJ, 13 February 1969, Case 14/68, *Walt Wilhelm*, para. 11; CJEU, 3 May 2011, Case C-375/09, *Tele2 Polska*.
26 ECJ, judgments of 29 June 2006, in Case C-289/04 P, *Showa Denko v Commission*, paras. 50–63 and in Case C-308/04 P, *SGL Carbon v Commission*, paras. 26–38.
27 For the case law interpreting the *ne bis in idem* principle as laid down in Art. 54 CISA, cf. judgments the following judgments by the CJEU: 11 February 2003, Joined Cases C-187/01 and C-385/01, *Gözütok and Brügge*, paras. 25–48; 10 March 2005, Case C-469/03, *Miraglia*, paras. 28–35; 28 September 2006, Case C-150/05, *Van Straaten*, paras. 54–61; 28 September 2006, Case C-467/04, *Gasparini and Others*, 2006, paras. 22–37; 11 December 2008, Case C-297/ 07, *Bourquain*, paras. 33–52; 22 December 2008, Case C-491/ 07, *Turanský*, paras. 30–45; 27 May 2014, Case C-129/ 14 PPU, *Spasic*, paras. 51–74.
28 CJEU, 9 March 2006, Case C-436/04, *van Esbroeck*, para. 36.
29 CJEU, *van Esbroeck*, *op. cit.* (n. 28), paras. 35–36.
30 CJEU, *Menci*, *op. cit.* (n. 9), paras. 35–36.
31 CJEU, *Menci*, *op. cit.* (n. 9), para. 35 with reference to van *Esbroeck*, *op. cit.* (n. 28), para. 36.
32 Ibid.
33 Ibid.
34 CJEU, 14 February 2012, Case C-17/10, *Toshiba Corporation and Others v Úřad pro ochranu hospodářské soutěže*.
35 CJEU, *Toshiba*, *op. cit.* (n. 34), para. 97.
36 CJEU, *Toshiba*, *op. cit.* (n. 34), para. 115.
37 CJEU, *Menci*, *op. cit.* (n. 9), para. 36.
38 As was the case in *Toshiba* of the second fine imposed by the Czech Competition Authority with respect to the period when the Czech Republic had not yet acceded to the EU.

Compensation for Unjustified Detention and the European Arrest Warrant

Florentino-Gregorio Ruiz Yamuza

This article sheds light on the compensation for unjustified detention that occurred while carrying out the European Arrest Warrant. First, the article exposes the reality of the lack of regulation of this matter and the necessity of having a normative reference at the level of the European Union. Second, it highlights the relationship between compensation and the fundamental rights of the detained person and therefore with the provisions of the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. Third, it outlines the frequently occurring difficulty of establishing the unjust or arbitrary nature of detention, especially when it comes to the enforcement of an extradition request. Fourth, the article describes some of the problems related to determining the Member State that should assume the compensation and reflects on the appropriate compensation procedure.

I. Compensation for Undue Detention – an Unsolved Problem

In the discussion on the EU's surrender regime – the Framework Decision on the European Arrest Warrant (hereinafter FD EAW) –, compensation in cases of undue detention as a consequence of the execution of an extradition request has not yet raised much interest or been considered a problematic issue).[1] Official documents have not dealt with this issue to a great extent. References and studies have limited themselves to stating that the need for compensation is a reality; however, it seems that they merely refer to the national sphere in

terms of eliciting an opportune response.[2] Consequently, the problems connected with this type of compensation have not attracted abundant attention in legal literature so far, without prejudice to the existence of some research that I will refer to in this article.

The issue of compensation poses specific challenges. Key concepts deserve a comprehensive approach, and the quest for realistic solutions must be aligned with the scheme of judicial cooperation within the EU's Area of Freedom, Security and Justice, with the doctrine of the European Court of Human Rights (ECtHR), and with the legal traditions of the Member States.[3] Several fundamental questions are still unanswered, such as: [4]

- Should unjust deprivation of liberty only cover situations in which the detained person is finally acquitted, or can other cases be included?
- Should compensation be granted only in cases of pre-trial detention, or is it also possible to grant it if an unjustified deprivation of liberty has occurred as a consequence of an EAW requesting the surrender of a person to serve a prison sentence passed in the issuing Member State?[5]
- Which Member State should be responsible for the compensation – the issuing State or the executing State?
- What procedure should be followed for compensation?

We will approach these questions in three steps: First, identifying the legal bases by which to establish the obligation to compensate (II.); in order to have a complete picture, this analysis will include references to the national level, briefly mentioning the Spanish legal system. Second, determining (within the casuistry of the EAW) when the deprivation of liberty can be tagged as unjustified (III.). Third, considering whether the obligation to compensate should be attributed to the issuing or to the executing Member State and which procedure is deemed appropriate (IV.). The article is rounded off with some concluding remarks, including my personal views on the problem (V.).

II. Legal Context

1. The supranational instruments

The FD EAW does not specifically provide rules on compensation for persons who have suffered unjustified detention in EAW cases. The regulation on expenses in Art. 30 FD EAW could be considered a possible legal basis, but this is debatable because of the wording, which is as follows:

> 1. Expenses incurred in the territory of the executing Member State for the execution of a European arrest warrant shall be borne by that Member State. 2. All other expenses shall be borne by the issuing Member State.

It is doubtful whether compensation for unjustified detention is covered by the concept of expenses. The notion of "expenses" seems instead to relate to costs inherent to the processing of the EAW, and, where appropriate, to the enforcement of the surrender. Thus, in the logic of the FD EAW, expenses are distributed according to where the costs have been incurred.

By contrast, compensation for unjustified detention is an enforceable right of the person who has suffered it and who is entitled to claim compensation from the State. Hence, even though the detention might occur in the executing Member State, it is indirectly related to the proceedings in the issuing State, in other words, the arrest is ultimately ordered on the basis of the requesting decision from the issuing Member State. Another disadvantage of using Art. 30 (1) FD EAW as a possible legal basis concerns situations in which the defendant is acquitted or the case is disposed of after the defendant's surrender to the issuing Member State. In these circumstances, it is not logical to assume responsibility on the part of the executing Member State for compensating the unjustified detention that took place in its territory due to the EAW.

Searching for a legal basis in relevant (implementing) national legislation is also not a successful approach. Although the Spanish Act 23/2014 on Mutual Recognition of Judicial Decisions in Criminal Matters in the EU (hereinafter AMR),[6] for example, contains some references to "compensation", they always refer to the compensation of victims of crime, third parties, or Member States for damages that might have been caused in conjunction with international cooperation (Arts. 15, 25, 173.2 b) and 3, 175.1, and 2 of the AMR). Further, the legal basis for the establishment of a compensation scheme for unjustified detention is found indirectly in supranational fundamental rights law to which the FD EAW, the Spanish AMR, and other acts transposing the FD EAW into the Member States' legal systems refer.[7]

In this context, Art. 6 TEU refers to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the Charter of Fundamental Rights of the European Union (CFREU), and the constitutional traditions of Member States – thus, a closer look at these instruments is necessary in order to find the applicable legal framework for the question of compensation at issue:

- Art. 5 ECHR sets out the right to liberty and security as well as the situations justifying the deprivation of liberty, including extradition detention (para. 1, letter f)). Para. 5 of Art. 5 ECHR explicitly guarantees the right to compensation for persons arrested in contravention of the provision of Art. 5 ECHR.
- Art. 6 CFREU briefly recognizes that "[e]veryone has the right to liberty and security of person." However, scope

and limitations of Art. 6 correspond to Art. 5 ECHR,[8] and Art. 52 (3) CFREU clarifies that the corresponding guarantees of the Charter have the same meaning and scope as those laid down in the ECHR. Consequently, the limitations that might legitimately be imposed on the right to liberty and security set out in the Charter cannot exceed those permitted by Art. 5 ECHR.

2. Compensation for unjustified detention in Spain

A proper understanding of compensation in cases of unjustified detention within the scope of the EAW requires, as pointed out above, an analysis both at the supranational and national levels. Considering that compensation mechanisms should be articulated through European Union law from a procedural point of view, the question remains which substantive legislation should be established on this matter. National laws can serve as a model; however, they are heterogenous regarding the viability and amount of compensation. In the following I outline the Spanish compensation system which, due to its originality and complexity, can illustrate, by way of comparison with other systems, the variety and heterogeneity of the possible regulations.

The Spanish Constitution[9] establishes the basis of the compensation system for losses caused by the activities of public officials and services, making a distinction between damages due to the (mis)functioning of public services (Art. 106.2)[10] and damages caused by judicial error (Art. 121)[11]. The Organic Act on the Judiciary specifies constitutional rules and explicitly addresses compensation for unjustified detention in its Art. 294:[12]

> 1. Individuals who have been under preventive imprisonment[13] and are subsequently absolved from the alleged charge (due to the non-existence of the fact they were accused to have committed) or if a non-suit writ has been issued with regard to those criminal proceedings may claim compensation, provided that they have sustained any damages therefrom. 2. Compensation will be determined considering the time they were remanded in custody and in view of the personal and family consequences […]

The scope of compensation under this precept is doubly restricted: first, it is limited to pre-trial detention situations; second, it is limited to those cases in which it cannot be proved that the actual event constituting a crime has occurred (non-existence of the fact). These limitations show that tackling compensation issues in the context of the EAW is very difficult, given that compensation rules differ from one Member State to another.[14]

However, the Spanish Constitutional Court and the Spanish Supreme Court developed a broader interpretation of this concept of compensation in Spanish law after and in light of several ECtHR judgments against Spain.[15] Accordingly, the principle of presumption of innocence should not be undermined by a legal framework (and case law) making compensation dependent on a previous decision not to prosecute or stop criminal proceedings or acquitting the accused person on the basis of the non-existence of the fact. There should be no qualitative difference between the acquittal or dismissal of a case on the grounds of insufficient evidence of the defendant's participation in an ontologically existing fact and in those situations in which the commission of the crime itself cannot be proved.[16]

In my view, this broader interpretation of Art. 294 by the highest Spanish courts is correct. In principle, any person deprived of his/her liberty in criminal proceedings should be compensated for the detention suffered if the case ends with an acquittal or a decision of dismissal. When the person's arrest takes place, he/she must be considered innocent (due to the legal presumption enshrined in Art. 6(2) ECHR, Art. 48(1) CFREU, and Art. 24.2 of the Spanish Constitution). In other words, considering that after the proceedings no guilt has been proven, the defendant had to be presumed innocent *before* the criminal proceedings were initiated and still has to be presumed innocent *after* the criminal case has been closed. Consequently, we can establish that an innocent person (a legal presumption that remains intact after the closing of the criminal proceedings) who has suffered imprisonment has the enforceable right to claim compensation.

This excursus into the Spanish compensation scheme shows that the diverging Member States' legislation on this matter can be aligned. In the Spanish case, jurisprudence overcomes the strict wording of the law and Spanish courts not only aligned their case law to the one of the ECtHR, but also bring the Spanish legal situation closer to other EU Member States. We can reasonably expect that this new case law forms the basis for smoother cross-border cooperation between Spain and other Member States in cases of unjustified detention within the framework of the EAW. This brings us to the next problematic issue, i.e. how the lawfulness of detention is assessed.

III. Assessing the Lawfulness of Detention

1. The ECtHR's case law

A prerequisite to determine the justification of compensation is the (un)lawfulness of detention. The assessment of this issue essentially necessitates a closer look at the ECHR. The ECHR provides a supranational model for national legislations. An analysis of the ECtHR's case law shows that the legitimacy of the deprivation of liberty can be affected by numerous factors, e.g. the excessive and disproportionate duration of depriva-

tion of liberty, the lack of detailed records on the reasons for or place of detention, the lack of effective judicial control of the deprivation of liberty, and the *a priori* impracticality of deprivation of liberty[17] – an issue that particularly concerns extradition.[18]

Moreover, equating unjust detention with a deprivation of liberty followed by an acquittal or dismissal of the case might become inaccurate, depending on a series of concurrent factors. Detention might be regarded as unjust in proceedings in which the defendant is ultimately acquitted or in which the case ends with a final dismissal, but these are not exhaustive hypotheses. If we assume that the acquittal of the defendant or the dismissal of the case are conditions for compensation, in extradition cases, it would invariably be the issuing Member State that should assume the compensation, once the procedure has been concluded. Such a conclusion is also consistent if one compares this situation with one that would apply when compensating those who have suffered pre-trial detention in national proceedings.

In principle, the detention has to fulfil at least one of the justification grounds listed in Art. 5 ECHR in order to be deemed fully legal. It should be recalled in this regard, that, despite their closeness in meaning, unjustified and unlawful detention are not the same thing, even though the terms might overlap and be used interchangeably.[19] At least from a theoretical point of view, they need to be distinguished, since nuances exist. When the Oxford Dictionary defines "unlawful" as "not conforming to, permitted by, or recognized by law or rules," its meaning is very close to that of illegal.[20] By contrast, the term "unjustified" is defined as "not shown to be right or reasonable"[21] or "not justified; not demonstrably correct or judicious; not warranted or appropriate."[22] In *extradition* cases, this distinction seems to be pertinent, and it seems that it is the guiding principle in the ECtHR's case law, particularly on Art. 5(1)(f) ECHR:[23]

In several judgements, the ECtHR has stated the following:

- Lawful arrest or detention of a person against whom action is being taken with a view to deportation or extradition "does not demand that detention be reasonably considered necessary, for example, to prevent the individual from committing an offence or fleeing. In this respect, Article 5 § 1 (f) provides a different level of protection from Article 5 § 1 (c): all that is required under sub-paragraph (f) is that 'action is being taken with a view to deportation or extradition'. It is therefore immaterial, for the purposes of its application, whether the underlying decision to expel can be justified under national or Convention law."[24]
- The term "action taken" is interpreted broadly in the sense that detention might be justified "[…] by enquiries from the competent authorities, even if a formal request or an order of extradition has not been issued, given that such enquires may be considered 'actions' taken in the sense of the provision."[25]
- The time element is considered to be of utmost importance. Accordingly, any deprivation of liberty is justified only as long as extradition proceedings are in progress. The ECtHR stated in this context: "If such proceedings are not prosecuted with due diligence, the detention will cease to be permissible under Article 5 § 1 (f)."[26]
- Consistency with the overall purpose of Art. 5 ECHR is key for the ECtHR as the means by which the Court links justification and lawfulness of detention in order to avoid arbitrary detention. Hence, in order to protect the individual against arbitrariness, deprivation of liberty must be "... closely connected to the ground of detention relied on by the Government; the place and conditions of detention should be appropriate; and the length of the detention should not exceed that reasonably required for the purpose pursued."[27]
- Lastly, the ECHR does not constrain or elaborate provisions concerning the circumstances in which extradition might be granted or regarding the extradition procedure; consequently, even atypical extradition might comply with the ECHR.[28]

2. The particular case of the Framework Decision on the European Arrest Warrant

The FD EAW operates according to the following rules: The requesting (issuing) Member State issues the EAW, generally in the form of an alert for the requested person entered into the Schengen Information System (SIS)[29]. Once the person sought is found in the territory of the requested (executing) Member State, the judicial authorities of both Member States cooperate to determine whether the surrender is feasible and coordinate the extradition proceedings. As a result, they apply different sets of rules: the national act of each having transposed the FD EAW, the FD EAW itself, and flanking frameworks, such as the CFREU, ECHR, and the national constitutions (see also above II.). In addition, national jurisprudence as well as the CJEU's and ECtHR's case law must be taken into account. Each particular situation requires close examination in order to conclude whether unjustified or unlawful detention existed and which Member State (the issuing or the executing one) should be deemed liable for such an infringement. Determining the suitability of compensation and the amount to be paid under the applicable law might imply specific challenges, as illustrated by the following:

a) Grounds for refusal

If, in accordance with Arts. 3 or 4 FD EAW, a decision was passed that denied the surrender of the person sought, this very

fact should not necessarily lead to the conclusion that the time the person spent in prison or under arrest constitutes unjustified or unlawful detention. The refusal of the requested surrender might have several reasons, and, quite often, assessing the viability of an EAW request takes time. In such a scenario, the deprivation of liberty suffered by the person sought while the extradition request was examined might be entirely lawful and justified or it may have been subject to the concurrent factors analysed supra under III.1. In the specific case of the EAW, we should further distinguish between a refusal on the basis of mandatory refusal grounds (as enshrined in Art. 3 FD EAW) and optional grounds for refusal (pursuant to Arts. 4 and 4a FD EAW).

If the executing judicial authority declares that extradition must be denied because of one of the refusal grounds in Art. 3 FD EAW, the question arises as to whether there has been an infringement of the rules governing justified and lawful detention pursuant to the supranational and national instruments and case law referred to above. Two scenarios are possible:

First, we can assume that the executing judicial authority carefully verified the circumstances foreseen in Art. 3 FD EAW and has diligently dealt with the extradition request. Accordingly, a warrant was issued following the requirements of the FD and said warrant was processed correctly and adequately. In this case, any hypothetical liability related to the unlawfulness of detention (and the compensation obligation arising from it) can only be established with the issuing Member State authority and only if such authority knew of the existence of the circumstances preventing the surrender in advance but still chose to issue the warrant.

Second, and conversely, if the intervention of the executing authority was slow, wrong, or inadequate, possible shared responsibility with the issuing Member State authority (in one of the cases I have just described above), can be determined. If the request was admissible, even the sole responsibility of the executing Member State may be established.

As for the optional grounds for refusal (Arts. 4 and 4a FD EAW), it is even more cumbersome to determine the hypothetical liability of the issuing Member State, given that there is a degree of uncertainty inherent in the listed refusal grounds. We should also bear in mind that, even though a Member State may have refused the extradition, another Member State may re-evaluate the EAW anew if, for instance, the same EAW is reissued and the same sought person has travelled to another Member State. In other words, the initial denial of the EAW by a Member State does not prevent the surrender from being affirmed by the executing authorities of a third Member State. In these cases, a possible solution for compensation might be found in Art. 26(1) FD EAW. According to this article, the time spent in detention in the executing Member State shall be deducted from the total detention period to be served in the issuing Member State as a result of a possible custodial sentence passed there. Hence, in a situation where there has first been a possibly unjustified detention period followed by a fully legal detention period that ultimately led to the surrender of the requested person, the most suitable solution would probably be the deduction of the total periods of detention suffered, i.e. both the justified and unjustified detention periods.

b) Fundamental rights as a refusal ground

A refusal of the EAW due to fundamental rights infringements may lead to problems analogous to those involving refusals on the basis of Arts. 3, 4, and 4a FD EAW. Likewise, proportionality-related issues may also give rise to problems.

Although not explicitly stipulated in the FD EAW as a refusal ground, the CJEU has recognized that the executing Member States may refrain from executing an EAW due to fundamental rights concerns.[30] Although the CJEU requires the executing authority to comply with several steps before it takes the granting decision, the executing authority of a Member State is entitled to deny surrender, having a certain margin of appreciation. Similar to the explicitly laid down refusal grounds described under a), also here a Member State may grant extradition in the future even though it had previously been denied by another Member State. It is still unclear whether refusals due to fundamental rights issues can result in compensation for the time spent in arrest while decisions on extradition had to be prepared and taken. Furthermore, the question again arises as to which Member State should assume the compensation.

It can be argued that the issuing Member State should be obliged to compensate, since the executing Member State refusing the surrender had to intervene in order to preserve fundamental rights. Nevertheless, this solution would create a disparity with the situation of other detainees in the issuing Member State who endure similar fundamental rights infringements (e.g. poor prison conditions) but are not entitled to compensation.

c) Other issues

Errors related to routine procedural matters, e.g. mistakes made in identifying the sought person, detentions and arrests of the wrong person for several days, and too lengthy or slow extradition proceedings, demand careful assessments to conclude which authority in which Member State was responsible for them. Another point in the discussion on paying compensa-

tion relates to situations in which the surrender is to be made subject to conditions (Art. 4a (1)(d), and Art. 5 FD EAW) but the required guarantees are not given by the issuing Member State in the end. Also, here, the time spent in prison in the executing Member State could equally be considered unjustified detention, even if the deprivation of liberty was initially legitimate.

IV. Member State to Assume the Obligation to Compensate and Compensation Procedure

The examples given under III.2 have shown that, in extradition cases, diverse situations exist in which unjustified detention may occur. In extradition cases, the proceedings are different from purely national criminal proceedings. In proceedings at the national level, the closure of the proceedings without a conviction occurs within a context that leaves less room for legal uncertainty, since the closure without conviction does not depend on future events, such as the decision of another State. This is different when detention is part of EAW/extradition proceedings: if a Member State executing an EAW refuses the surrender, this decision does not imply final procedural closure, since the person concerned can be subsequently handed over to the issuing State, on the basis of the same facts, by another Member State or by a third State outside the European Union. Theoretically, the likelihood of reopening the case could impede a possible compensation for unjustified detention. Moreover, unjustified detention might happen again after a conviction in the issuing Member State. This is very unlikely to happen in national cases (although it is possible, for instance, that imprisonment after the penalty imposed is statute-barred), but it could occur in extradition proceedings when two States are involved and the executing Member State considers the surrender to be denied by applying the grounds for refusal laid down in the FD EAW (Arts. 3, 4, 4a 1. a), b) or c)). I propose a system that obviates a debate each time a decision needs to be taken as to which Member State should be responsible for compensation for unjustified detention in EAW cases. This system could be organised as follows:[31]

- The compensation process would consist of two phases: first, determining the existence of unjustified detention and, second, setting and paying the amount to be compensated. I advocate that both determining the existence of unjustified detention and determining the amount to be paid should be carried out in the Member State where the detention has been verified. This Member State should take the decision by applying its own law. It should be taken regardless of the final grounds substantiating the conclusion that the detention was unjustified. Such an approach would ensure legal certainty, since the person concerned can rest assured that the Member State in which the detention occurred bears responsibility for the compensation, regardless of the reasons for the illegality of the arrest and where they originated (in the State of detention or another State).
- Compensation should normally be borne by the executing Member State in whose territory the initial deprivation of liberty occurred and should cover the period spent under arrest until the moment of effective surrender to the issuing State. If an unjustified arrest continues after surrender, the obligation to compensate should shift to the requesting State from that moment on. This is a neat and simple solution, and it would also apply if the unjustified detention was initially caused by an error or a deficiency in the executing State (the wrong person was surrendered or the executing authority failed to apply a refusal ground, e.g. time limitation).
- Conferring the obligation to compensate to the State in which the deprivation of liberty occurred could be accompanied by an indemnity clause covering the hypothesis that the arrest lacked justification, namely that it was not caused in the State in which the deprivation of liberty had taken place. On the one hand, this approach could indeed lead to litigation, taking into consideration the different opinions Member States may have on the issue of compensation. On the other hand, the approach would be in line with compensation schemes in other cooperation instruments that stipulate, for instance, that the EU Member States can share both the costs and benefits derived from international judicial cooperation.[32]
- In cases in which a first decision denies extradition and subsequent surrender of the same person by another Member State in another EAW proceeding occurs in relation to the same facts, the concept of Art. 26 FD EAW should be preferentially applied (see above III.2a). Instead of compensating the unjustified deprivation of liberty that occurred due to the first EAW, the detention time should be deducted in the subsequent proceedings that ultimately led to the surrender.
- Considering the possible issuance of successive EAWs for the same offence and given what we have just concluded, the compensation procedure should begin once a final decision has been reached in the issuing State acquitting the requested person or dismissing the case.
- Depending on which Member State might be found liable for the losses caused by the unjustified detention (issuing or executing State or even both of them), the compensation procedure would need to be different. In addition, we must consider situations in which the compensation for unjustified detention might be claimed for a Member State other than that of the residence of the affected person, e.g. in the event that the person who suffered unjustified detention did not claim compensation when he/she was in the State in which the arrest occurred and decides to claim it once he/she

is back in his/her home country.[33] Here, a scheme similar to the scheme to compensate victims of crime in cross-border situations, as set out in Directive 2004/80/EC,[34] could be adopted. This Directive ensures that each EU country has in place a national scheme that guarantees appropriate State compensation to victims of intentional violent crimes. It also ensures that compensation is easily accessible, regardless of where in the EU a person becomes the victim of a crime. It could even be considered that the Member State of the nationality/residence of the person who has suffered unjustified detention take over the compensation process and the pertinent award payment, claiming reimbursement from the Member State considered ultimately responsible for compensation.

V. Concluding Remarks

The compensation of unlawful or unjustified deprivation of liberty in cross-border cases involving the European Arrest Warrant might not be at the top of the agenda of problems to do with the mutual recognition instrument. It deserves deeper reflection, however, and demands a univocal approach at the European Union level. In synthesis of the ideas presented in this article, the following recommendations are relevant:

- The EU should establish a unitary legal framework that sets out compensation for unjustified detention in EAW cases and the procedure to obtain such compensation.
- This legal framework should define the cases in which compensation for unjustified deprivation of liberty can be obtained as a consequence of the execution of an EAW.
- The framework should guarantee that any person who has suffered an unjustified deprivation of liberty has access to a compensation system. This system must harmonize the situations giving raise to compensation, determine which Member State would be a priori responsible for compensation, and define a procedural pattern of claim, when it comes to the operation of EAWs.
- The system must legally clarify whether compensation in transnational cases should only cover cases in which there has been an acquittal or dismissal concerning the arrested person or whether it should be extended to other scenarios where there has been a deprivation of liberty not followed by a conviction.
- In addition, a debate about a possible procedural model that would meet the identified needs must be launched.
- The lack of regulation in this matter should be remedied as quickly as possible in order to provide sound legal footing – one on which the victims of unlawful detention can stand.

Dr Florentino-Gregorio Ruiz Yamuza
Senior Judge of the Appeal Court of Huelva (Spain). Member of the Spanish Judicial Network for International Cooperation (REJUE), Criminal Division

1 Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA), *O.J.* L 190, 18 July 2002, 1.

2 Cf., for instance, the European Parliament Report on the implementation of the European Arrest Warrant and the surrender procedures between Member States (2019/2207(INI) which does not mention this issue The report is available at <https://www.europarl.europa.eu/doceo/document/A-9-2020-0248_EN.pdf>. Similarly, the European Commission Handbook on how to issue and execute a European Arrest Warrant (*O.J.* C 335, 6 October 2017, 1), has only one reference to compensation at p. 36: "Following the surrender of the requested person, the issuing Member State must take into account the periods of detention that have resulted from the execution of the EAW. All of these periods must be deduced from the total period of the custodial sentence or detention to be served in the issuing Member State (Article 26 of the Framework Decision on EAW). If the person is acquitted, provisions of the issuing Member State on compensation for damages may apply." The study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, deals with the matter to some extent, dedicating its section 6 (pp. 123 et seq.) to the different national compensation schemes for the case of unjustified detention and its relationship with international judicial cooperation. The study is available at <https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604977>. All hyperlinks referred in this note and the subsequent notes were accessed on 26 November 2021.

3 On the need for regulation in this field, see the European Parliamentary Research Service paper "*Revising the European Arrest Warrant. European Added Value Assessment accompanying the European Parliament's Legislative own-Initiative Report (Rapporteur: Baroness Ludford MEP)*", <https:// www.europarl.europa.eu/RegData/etudes/etudes/join/2013/510979/IPOL-JOIN_ET(2013)510979_EN.pdf>. See also V. Costa Ramos, "Future procedural rights in the context of the European Arrest Warrant, pre-trial detention and detention", <https://carlospintodeabreu.com/wp-content/uploads/2020/10/Costa-Ramos-The-next-steps-Detention-and-EAW-V3.pdf>.

4 My personal interest in this matter started when I had the pleasure of participating in the European Judicial Network project "Compensation for unjustified detention in EAW-cases", which ended in September 2017, <https://www.ejn-crimjust.europa.eu/ejnupload/RM17/NL_Report_Regional_2017.pdf>.

5 On broaching the need for regulation on pre-trial detention at the EU level, see E. Baker, T. Harkin, V. Mitsilegas, and N. Persak, "The Need for and Possible Content of EU Pre-trial Detention Rules", (2020) *eucrim,* 221; A. Martufi and C. Peristeridou, "Pre-trial Detention and EU Law: Collecting Fragments of Harmonisation Within the Existing Legal Framework", (2020) 3 *European Papers*, 1477.

6 Act 23/2014 of 20 November 2014, on Mutual Recognition of Judicial Decisions in Criminal Matters in the European Union, *Official Gazette (BOE),* 21 November 2014. The English version of this Act (translated by the Spanish Ministry of Justice) is available at <https://ejn-crimjust.europa.eu/ejnupload/InfoAbout/English%20version%20LAW%2023%20of%202014.pdf>.
7 Cf. Recital 12 and. Art. 1(3) FD EAW. By the same token, Art. 3 AMR, entitled "Respect for fundamental rights and liberties", reads: "This Act shall be applied respecting the fundamental rights and liberties and the principles set forth in the Spanish Constitution, in Article 6 of the European Union Treaty and the Charter of Fundamental Rights of the European Union, and in the European Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe of 4 November 1950."
8 Explanations relating to the Charter of Fundamental Rights, *O.J.* C 303, 14 December 2007, 2.
9 Constitution of 31 October 1978, *Official Gazette*, 29 December 1978. Its English version is available at <https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf>.
10 The wording is as follows: "[…] Private individuals shall, under the terms established by law, be entitled to compensation for any loss that they may suffer to their property or rights, except in cases of force majeure, whenever such loss is the result of the operation of public services."
11 This right reads as follows: "[…] as well as those arising from irregularities in the administration of justice shall give rise to a right to compensation by the State, in accordance with the law."
12 Organic Act 6/1985 of 1 July on the Judiciary, *Official Gazette*, 2 July 1985. An English translation of the Organic Act is available at <https://www.poderjudicial.es/cgpj/es/Temas/Compendio-de-Derecho-Judicial/Leyes/Ley-Organica-6-1985--de-1-de-julio--del-Poder-Judicial>.
13 Literally translated from "prisión preventiva" and can be understood as pre-trial detention.
14 The Spanish model is complex, since the compensation foreseen for unjustified detention and for judicial error are more restrictive than the general scheme of compensation for losses stemming from the functioning of public services. Art. 106.2 of the Spanish Constitution, and Act 40/2015 of 1st of October on the Legal Regime of the Public Sector (*Official Gazette*, 2 October 2015, <https://www.boe.es/eli/es/l/2015/10/01/40>) contemplate general coverage for losses connected with the functioning of public services, disregarding any degree of negligence that may have been produced: "Individuals have the right to be compensated by the relevant Public Administrations for any loss suffered in their property and rights, provided that such loss is a consequence of normal or abnormal functioning of the public services except in cases of force majeure or damages the individual has the legal duty to tolerate in accordance with the Law." Conversely, Arts. 293 and 294 of the Organic Act on the Judiciary make compensation in cases of judicial error and for unjustified detention dependent on a sort of malfunctioning of the justice system.
15 ECtHR, 25 April 2006, *Puig Panella v Spain,* Appl. no. 1483/02; ECtHR, 13 July 2010, *Tendam v Spain,* Appl. no. 25720/05; ECtHR, 16 February 2016, *Vlieeland Boddy and Marcelo Lanni v Spain*, Appl. no. 53465/11.
16 Spanish Constitutional Court, judgments 8/2017, 19 January 2017, ECLI:ES:TC:2017:8; 10/2017, 30 January 2017, ECLI:ES:TC:2017:10, and 85/19, 19 June 2019, ECLI:ES:TC:2019:85; Spanish Supreme Court, Judicial Review Chamber, decision 1348/2019, 10 October 2019, ECLI:ES:TS:2019:3121.
17 ECtHR, 12 June 2008, *Shchebet v Russia,* Appl. no. 16074/07; ECtHR, 2 October 2008, *Rusu v Austria,* Appl. no. 34082/02; ECtHR, 12 February 2009, *Nolan and K. v Russia*, Appl. no. 2512/04; ECtHR, 7 June 2007, *Garabayev v Russia*, Appl.no. 38411/02. See also the ECtHR judgments cited in n. 15.
18 The ECtHR "*Guide to Article 5 of the Convention*" also offers detailed explanations on how to construe the "lawfulness of detention under Article 5 § 1" (cf. part II of the guide) and "authorized deprivations of liberty under Article 5 § 1" (part III). The guide is available at <http://www.echr.coe.int/Documents/Guide_Art_5_ENG.pdf>.
19 The United Nations Human Rights Council resorts to the term "arbitrary" as something being more than merely against the law, interpreting the term widely to include such elements as inappropriateness and injustice (See, among others, *A v Australia*, Communication No. 560/1993; reaffirmed in *Danyal Shafiq v Australia*, Communication No. 1324/2004). The notion of arbitrariness is also used by the ECtHR: ECtHR, 29 January 2008, *Saadi v United Kingdom*, Appl. no. 13229/03; ECtHR, 26 April 2007, *Gebremedhin v France,* Appl. no. 25389/05; ECtHR, 10 May 2007, *John v Greece,* Appl no. 199/05).
20 <https://en.oxforddictionaries.com/definition/unlawful>. Cf. also the entry in Merriam Webster Legal Dictionary: "Not lawful, illegal", <https://www.merriam-webster.com/dictionary/unlawful#legalDictionary>.
21 Oxford Dictionary, *op. cit.* (n. 20).
22 Merriam Webster Dictionary, *op. cit.* (n. 20).
23 The following summarises the ECtHR's *Guide to Article 5 of the Convention, op. cit.* (n. 18), paras. 146 et seq.
24 ECtHR, 15 November 1996, *Chahal v the United Kingdom,* Appl. 22414/93, para. 112; ECtHR,5 February 2002, *Čonka v Belgium,* Appl. 51564/99, para. 38; ECtHR, 11October 2007, *Nasrulloyev v Russia*, Appl. 656/06, para. 69; ECtHR, 23 October 2008, *Soldatenko v Ukraine,* Appl. 2440/07, para. 109.
25 Commission decision of 9 December 1980, *X. v Switzerland*, Appl. no. 9012/80.
26 ECtHR, 19 February 2009, *A. and Others v the United Kingdom,* Appl. 3455/05, para. 164; ECtHR, 12 February 2003, *Amie and Others v Bulgaria,* Appl. 58149/08, para. 72.
27 *Ibid.* See also ECtHR, 20 December 2011, *Yoh-Ekale Mwanje v Belgium*, Appl. 10486/10, paras. 117–19 with further references.
28 ECtHR, 12 March 2013, *Öcalan v Turkey*, Appl. 46221/99, para. 86; ECtHR, 21 June 2011, *Adamov v Switzerland*, Appl. 3052/06, para. 57.
29 Cf. Arts. 9 and 10 FD EAW.
30 CJEU, 5 April 2016, Joined Cases C-404/15 and C-659/15 PPU, *Aranyosi and Căldăraru*; CJEU, 25 July 2018, Case C-220/18 PPU, *ML*; CJEU, 25 July 2018, case C-216/18 PPU, *LM*; CJEU, 15 October 2019, Case C-128/18, *Dorobantu*.
31 An EU-wide problem requires unified solutions a the Union level combining a common framework plus the application of national legislations, see H. Sørensen, Mutual recognition and the right to damages for criminal investigations, (2015) 5 *European Criminal Law Review*, 194–208.
32 See Art. 13 of Council Framework Decision 2005/214/JHA of 24 February 2005 on application of the principle of mutual recognition to financial penalties, *O.J.* L 76, 22 March 2005, 16: "Monies obtained from the enforcement of decisions shall accrue to the executing State unless otherwise agreed between the issuing and the executing State, in particular in the cases referred to in Article 1(b)(ii)."
33 For the peculiarities of having two Member States involved in the compensation process, see also H. Sørensen, "International and European Approaches to Extraterritorial Liability for Violation of Fundamental Rights in International Criminal Law", in: W. Benedek, F. Benoit-Rommer, W. Karl, and M. Ketterman (eds.), *European Yearbook on Human Rights,* 2013, 1.
34 Council Directive 2004/80/EC of 29 April 2004 relating to compensation of crime victims, *O.J.* L 261, 6 August 2004, 15.

Report

Strengthening of International Cooperation in Criminal Matters: Extradition and Mutual Legal Assistance

Report of the Council of Europe Online Conference – 5 May 2021

On 5 May 2021, the Council of Europe's Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC) hosted an online conference under the auspices of the German Presidency of the Council of Europe (CoE). It had the aim of strengthening international cooperation in criminal matters. Erik Verbert, president of PC-OC, delivered the welcome address, which was followed by opening speeches from Jan Kleijssen, director of the CoE's Directorate of the Information Society and Action against Crime, and Dr. Margaretha Sudhof, State Secretary of the German Federal Ministry of Justice and Consumer Protection. During the morning session, the conference consisted of insightful expert interventions on current issues in mutual legal assistance (MLA). The afternoon session was devoted to extradition and split into three workshops held in parallel. Member States and representatives from third countries engaged in productive discussions and a valuable exchange of views.

I. MLA: Cooperation between CoE and EPPO

After an introduction to the European Public Prosecutor's Office (EPPO), explaining both its structure and remit, current challenges were addressed. The EPPO is able to render MLA if it is already in possession of relevant information or evidence, but it can neither extradite persons nor ask for a surrender or an extradition. Safe communication within the EPPO and between delegated prosecutors in the EU Member States was identified as a crucial issue. An alternative to encrypted emails – which no longer meet contemporary standards – could be a secure cloud. This solution would allow for sharing of documents and enable safe communication between the EPPO members.

An outlook into the future of the office included plans to extend the competence of the EPPO to terrorism and to create a European criminal court. The discussion was marked by scepticism concerning the necessary specialisation of the prosecutors and the sensitivity of the area of state protection. One obstacle to the establishment of a European criminal court was seen in Art. 86 TFEU, which does not provide for such an extension, making amendments to the EU treaties necessary.

Next, the legal framework for cooperation between third countries (both within and outside the CoE) and the EPPO was presented. With regard to the rule of speciality, the issue of transfer of evidence was raised. If MLA is provided to a European delegated prosecutor or the EPPO, state authorities must be made aware that the EPPO has access to the information in its entirety and that evidence will be presented to the court competent in the specific matter. This competence may differ from the jurisdiction originally assumed when MLA was requested. The responding state could, however, make the provision of evidence subject to the condition that no such transfer takes place. In this case, the country in which the trial is conducted would have to send a new request to the responding state. If no such condition is imposed, the EPPO may use evidence where it is needed.

Another issue within the context of cooperation between third countries and the EPPO concerned the interpretation of Art. 104 (6) of Regulation (EU) 2017/1939 ("the EPPO Regulation"), which states that both sides must mutually support each other. The question was raised as to whether this includes the possibility of exchanging information spontaneously, for example if the EPPO seizes a computer and coincidentally finds evidence of other crimes outside its jurisdiction. As it is committed to the principle of legality, the EPPO would have to inform the relevant authorities in the event of such findings.

Switzerland gave its perspective, namely that at the international level a legal basis for cooperation with the EPPO has been lacking. It would hence be supportive to create a new legal instrument for cooperation with the EPPO within the framework of the CoE. A representative of the US Department of Justice announced that US authorities will cooperate with the EPPO as well as the Department's intention to render MLA when requested.

In the ensuing debate, the conference participants discussed the following:

- Whether the courts that hear EPPO cases may be considered EU courts (and cases cannot be considered national), or:
- Whether EPPO procedures remain national, since they follow national requirements with national prosecutors before national courts.
- The latter approach is particularly questionable if proceedings would eventually be heard before a European criminal court sometime in the future. In this case, the current system would have to be revised, but it seems likely that the EPPO would still use national structures.

II. Extradition

1. Effects of detention conditions on extradition

The first workshop analysed the legal basis in extradition cases, addressing the effects of detention conditions in the requesting state on extradition.

First, the approach of the European Court of Human Rights (ECtHR) to detention conditions was discussed. Since *Soering v UK*,[1] a CoE member state could be in breach of a convention right when surrendering an individual if the authorities had been aware that that person may be subject to inhuman treatment in the requesting state. This decision motivates states to examine the conditions in another (non-member) state. A summary of the principles and requirements for detention facilities can be found in *Muršić v Croatia*.[2]

Secondly, the relevant legal framework of the EU and the authoritative interpretation of the law of the Court of Justice of the European Union (CJEU) were presented. The case *Aranyosi and Căldăraru*[3] was cited as having changed the legal landscape: in certain cases, it became imperative for executing EU Member

States to assess detention conditions in the issuing state before surrendering the person requested.

This case law has had far-reaching consequences with regard to the numerous challenges encountered by practitioners. In particular, delays resulted because of the executing state's duty to assess the conditions in the issuing state. One of the difficulties is determining the detention facility in which the person will eventually be detained and finding objective, reliable information on that facility. Concerns were raised about the usefulness of reports drafted by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment, as their publication could be rejected by countries that do not agree with its content. Another point of discussion was whether a person extradited on the basis of assurances could be transferred to a prison with worse prison conditions upon the request of the person himself/herself, even though this would mean a breach of assurances.

Yet another problematic issue that was discussed concerned the different approaches by judicial authorities towards both the type of information requested and the structuring of information being sent back to the executing judicial authorities. The lack of a common understanding of acceptable minimum standards for detention conditions and the lack of consensus on what constitutes sufficient information or assurance leave a wide margin of discretion to national courts.

The issue of discriminatory treatment of prisoners was also raised. A person that is being transferred has to be treated in line with EU human rights standards, but prisoners not subject to EU cross-border instruments do not necessarily benefit from these standards.

Possible solutions include the development of a common methodology and common criteria for the assessment of detention conditions. The EU Agency for Fundamental Rights' Criminal Detention Database, which contains information on detention facilities in Member States that is objective, reliable, specific, and properly updated, could help in assessing prison conditions. Having a similar database within the CoE on the basis of the 1959 European Convention on MLA would also be useful. With regard to financial support for member states with inadequate prison conditions, it was left open as to how this could be financed. Reducing detention altogether and finding alternative cooperation methods other than the hard-to-monitor assurances could be a further part of the solution.

2. Effects of CJEU case law on extradition

The second workshop addressed the CJEU's case law and its effect on extradition. In the *Petruhhin* case,[4] the CJEU introduced the obligation to carry out a consultation procedure between the requested EU Member State and the EU Member State of nationality of the EU citizen being sought by a third country. The CJEU stated that it would constitute unequal treatment and a restriction of freedom of movement if an EU Member State does not extradite its own citizens but extradites those of another EU Member State. A justification for this restriction could be prevention of the risk of impunity. However, the CJEU has found that European criminal law provides for more proportionate means, such as a surrender to the state of nationality by means of an EAW and that this instrument is to be given priority over the extradition request of the third country. When discussing the *Petruhhin* judgment, the question arose as to how the decision should be applied in individual cases, i.e. what kind of information should be provided.

In the *Raugevicius* case,[5] the CJEU confirmed that the *ne bis in idem* principle may be an obstacle with regard to persons who are subject to an extradition request. The CJEU maintains that those persons should serve their sentences in the Member State of their nationality in accordance with the 1983 CoE Convention on the Transfer of Sentenced Persons, with an exception for long-term residents, who should also be able to serve their sentence in the requested state.

Lastly, reference was made to two recent cases. Case C-505/19 (*WS v Germany*), pending at the time, concerns the scope of the *ne bis in idem* principle within the Schengen area and its relation to Interpol red notices from third countries; the opinion rendered by the Advocate General was welcomed.[6] Case C-398/19 *(BY)*[7] was presented to show the possibility of extraditing a person to a third country if that person is a national of another EU Member State and if the other state does not issue an EAW in a reasonable time.

In the context of the US perspective, concerns were raised with regard to the development of the case law of the European Court of Justice on extradition. The participation of a non-Member State in CJEU proceedings is not provided for in the court's rules of procedure. The USA would neither be allowed to see written submissions of the disputing parties nor participate in the proceedings, whereas the US Supreme Court is open to the participation of other states. The role of the European Commission (EC) was also criticised. The EC would usually participate in all extradition cases before the CJEU. When asked to extradite a person to a Member State, the USA would do everything in its power to facilitate the extradition. Before the CJEU, however, the EC would intervene for the sake of harmonising EU law, taking an unfavourable stance towards extradition. Therefore, the USA wishes to enter into a dialogue with the EC before it takes a position before the CJEU that might affect the USA.

Another issue put forward by the USA concerns the obligation for EU Member States to treat citizens of other Member States like their own nationals. If the state of nationality asks for the return of a person, this state receives priority according to the *Petruhhin* mechanism. If the state does not extradite its own nationals, there is no way for the USA to have the person extradited. The USA is also concerned about the *ne bis in idem* rule: if a person has been prosecuted in an EU Member State and then travels to another Member State, *ne bis in idem* applies and the person cannot be extradited. This would have an adverse effect on extradition. In the extraditions treaties the USA has with different Member States, previous prosecution in the requested state only is laid down as one reason for a refusal to extradite. The CJEU created grounds for refusal, however, that the USA did not agree to, amounting to a breach of *pacta sunt servanda*. The US extradition treaty with the EU does not state, namely, that a ground for refusal would be the prosecution of the requested person in another EU state. In conclusion, the USA would like to engage in a dialogue with the EU on whether there is a way to bring the considerations of third states before the CJEU and work together with the EC and the Member States in order to apply their extradition treaties.

Next, the joint report of Eurojust and the European Judicial Network (EJN) on the extradition of EU citizens to third countries[8] was presented. The aim of the report was to gather information on the practical experience of national judicial authorities

in the area of extradition to third states and to identify the most relevant issues in this regard. The EJN and Eurojust identified uncertainties as to the scope of the CJEU's case law with regard to the Member States' obligations on extradition as well as practical and legal issues concerning the consultation procedure, such as:

- The identification of competent authorities in the Member State of nationality;
- Time limits for prosecution;
- Questions of jurisdiction or conflicts stemming from obligations under EU law versus those from extradition treaties;
- The results of the consultation procedure, which often do not lead to the prosecution of the person in his/her state of nationality.

Eurojust underlined its readiness to help identify competent authorities, to speed up the process, and to clarify the practical and legal extradition issues the Member States are facing. With regard to the consultation procedure, it was clarified that this obligation only arises if there is a legal basis for extradition, if the requested Member State prohibits the extradition of its own nationals, and if the requested person made use of the right to free movement.

Representatives from several CoE member states participated in the discussion that followed, expressing their reservations about the *Petruhhin* judgement. The Netherlands and Portugal claimed that the *Petruhhin* case was not the correct way to handle the situation in question. There will always be cases where issuing an EAW is not possible, rendering the Member State unable to protect its own citizen. According to Israel, the judgment widens the scope to non-extradition of a fugitive requested by a third state. Reciprocity in terms of extradition would be merely theoretical, because third countries would extradite while EU Member States would not. Finland interjected that the scope of application of the *Raugevicius* decision is narrow. The problem is that states need the requesting state's permission to enforce the sentence of the person in their own state and such permission is not always granted.

It was also put forth that the EC has no role in extradition cases, as extradition lies within the competence of the EU Member States. The US representative claimed that the decision in *Pisciotti* (the first extradition case involving the USA)[9] was wrong, as it ignored the extradition agreement between the USA and the EU.

The importance of improving the dialogue between the EU and third countries was once again highlighted. The similarity between US extradition requests and EAWs would be striking, and it was surprising that the CJEU violates international law by establishing a priority for EAWs. There were no positive interventions regarding the *Petruhhin* decision, which is lacking guidance on how to apply it. Third countries will be confronted with the negative effects of EU law and are lacking any possibility to intervene in proceedings before the CJEU. In conclusion, further clarification through CJEU judgments on the extradition of EU citizens to third countries would be helpful for practitioners.

3. Lessons learned from the COVID-19 pandemic

In the third workshop, three expert presentations shed light on the effects of the COVID-19 pandemic on international cooperation in criminal matters. The need for a comprehensive digitalisation of international cooperation in criminal matters was identified as the main lesson learned. The use of digital solutions, e.g. to transmit requests electronically, should not be limited to times of crisis but instead become the new norm. From the perspective of the United Nations Office on Drugs and Crime (UNODC), a broad variety of technical solutions is already available that can ensure the secure electronic transmission of requests, including secure platforms created by judicial bodies or bilateral/multilateral channels between states.

Eurojust reported on its work, which involves regularly updating the information received and making it available to practitioners. This includes a casework report for practitioners[10] and a compilation of information, gathered together with the EJN, on the impact of COVID-19 on cooperation in criminal matters in the EU.[11]

With respect to surrender procedures, the issuing of EAWs continued largely as usual throughout the pandemic. A prioritisation (e.g. of serious cases) took place in some Member States. As regards the execution of EAWs, confinement measures led to delays and difficulties regarding the actual surrender of requested persons. In many cases, Eurojust served as a go-between channel in negotiations between states, for example to reach an agreement on new surrender dates. With respect to the legal dimension of delays caused by the pandemic, the FD EAW allows for exceptions from the time limits set, but there is still uncertainty over which of the following provisions applies:

- Art. 17(7) ("exceptional circumstances");
- Art. 23(3) ("circumstances beyond control");
- Art. 23(4) ("serious humanitarian reasons").

Eurojust also noted that Member States regularly request supplementary information on conditions in the issuing state according to Art. 15(2) FD EAW, e.g. regarding quarantine measures.

A study conducted by the international cooperation network Red de Cooperación Penal Internacional (REDCOOP), which resulted in the drafting of a guide on good practices developed by the Ibero-American Association of Public Prosecutors (AIAMP), was presented.[12] The study highlighted that electronic transmission of requests was much more efficient for both MLA and extradition, saving both time and money, while at the same time being at least as secure as the paper-based process. Measures to further increase transmission safety should include the use of institutional e-mail addresses, instead of personal e-mail addresses. The use of electronic signatures was also recommended to ensure that the identity and content of the message remain unaltered, thereby securing the authenticity of a request. This means of transmission is considered compatible with international law, as it has not been prohibited by any conventions. Some conventions even encourage the use of electronic transmission, e.g. Art. 25 of the Budapest Convention. Some states already allowed and started using electronic transmission years before the pandemic. One example of a current regional instrument is the Treaty of Medellin.

Sometimes, judges had to release persons from extradition custody because of the uncertainty over when borders would reopen, and surrender could take place. Sanitary measures, which require proper coordination, were also mentioned as an important aspect of protecting the person and officers concerned.

The discussion afterwards touched upon digitalisation, in general, and the technical and legal issues surrounding the

electronic transmission of requests, in particular. Data protection was a major concern. A system based on a cloud can be problematic because the storage of information would be in the hands of the cloud provider. One possible solution would be the use of bilateral or multilateral channels that cannot store information but only digitally transmit the data. Ordinary e-mail would even be possible using encryption systems and commercial authenticity certification systems. To facilitate this, the provider needs to be registered in the state in which it is operating. Some argued in favour of digitalisation because there are no conventions at the international level explicitly requiring requests to be transmitted by mail or by courier. Paper-based documents do not grant any greater reliability than electronic transmissions, as signatures can be falsified. As a basis for future electronic transmission, it would be useful to start looking at domestic case law, where courts have accepted evidence gathered abroad and transmitted it digitally.

It was agreed that there is no "one-size-fits-all" solution but that solutions instead have to be developed on a case-by-case basis through direct consultations between the authorities involved. Detention prior to extradition was mentioned as being a key issue. It was reiterated that a surrender should be carried out as soon as possible (e.g. by land instead of by air or by using military aircraft), whenever possible. The time a person spends in extradition detention must be limited. Alternatives to detention that are less prejudiced to the requested person's fundamental rights but similarly effective should be explored, including house or night arrest.

III. Outlook for the Future of International Cooperation in Criminal Law

After the CoE conference, the CJEU delivered its judgment in Case C-505/19, *WS v Germany,* on 12 May 2021.[13] Essentially following the opinion of the Advocate General, the CJEU decided that extradition is part of law enforcement in the requested state and therefore covered by *ne bis in idem*. Treaties with third countries cannot interfere, as they are inapplicable if they contain obligations that are not in line with EU law. The judgment calls for a legal remedy that allows the person affected to obtain a final judicial decision establishing that the *ne bis in idem* rule applies. This decision still requires implementation in most EU Member States.

Primary EU law supersedes any bilateral international treaties contradicting EU law. If necessary, these treaties need to be amended in order to strengthen cooperation with third countries and to restore trust in international cooperation in criminal matters on the basis of treaties.

In regard to the digitalisation of international judicial cooperation, existing instruments often already allow for electronic submission, but countries do not always make use of this possibility in practice or even accept only paper-based requests. The solution could be the initiative launched by the European Commission to modernise cross-border judicial cooperation in the EU.[14] This initiative included a public consultation (that was open for feedback until mid-May 2021), which aims to make digital judicial cooperation the default option by means of a legislative proposal by the end of the year.

Lennard Breulich

---

1 ECtHR, 7 July 1989, *Soering v United Kingdom*, Applic. no. 14038/88.
2 ECtHR, 20 October 2016, *Muršić v Croatia*, Applic. no. 7334/13.
3 CJEU, 5 April 2016, Joined Cases C-404/15 and C-659/15 PPU, *Aranyosi and Căldăraru*; see also *eucrim* 1/2016, 16.
4 CJEU, 6 September 2016, Case C-182/15, *Petruhhin*; see also *eucrim* 3/2016, 131.
5 CJEU, 13 November 2018, Case C-247/17, *Raugevicius*; see also *eucrim* 4/2018, 203–204.
6 AG *Bobek*, Opinion of 19 November 2020 in Case C-505/19, *WS v Germany* (see also *eucrim* 4/2020, 287–288).
7 CJEU, 17 December 2020, Case C-398/19, *BY*; see also *eucrim* 4/2020, 289.
8 <https://www.eurojust.europa.eu/joint-report-eurojust-and-ejn-extradition-eu-citizens-third-countries>; see also *eucrim* 4/2020, 288. All hyperlinks referred to in this article were accessed on 1 October 2021.
9 CJEU, 10 April 2018, C-191/16, *Pisciotti v Germany*; see also eucrim 1/2018, 29.
10 <https://www.eurojust.europa.eu/impact-covid-19-judicial-cooperation-criminal-matters>.
11 <https://www.ejn-crimjust.europa.eu/ejn/EJN_DynamicPage/EN/86>; see also the article by Radu/Ernest, *eucrim* 2/2021, 114–116.
12 Available in Spanish only: <http://www.aiamp.info/index.php/grupos-de-trabajo-aiamp/cooperacion-juridica-internacional/documentos/buenas-practicas-de-los-miembros-de-la-aiamp-ante-covid-19>.
13 See also *eucrim* 2/2021, 100–101.
14 <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/digitalisation-justice/digitalisation-cross-border-judicial-cooperation_en>.

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

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, Vienna University of Economics and Business; Anna Pingen, Max Planck Institute for the Study of Crime, Security and Law, Freiburg; Cornelia Riehle, ERA, Trier
Editorial Board: Prof. Dr. Lorena Bachmaier, Complutense University Madrid, Spain; Peter Csonka, Head of Unit, DG Justice and Consumers, European Commission Belgium; Prof. Dr. Esther Herlin-Karnell, University of Gothenburg, Sweden; Mirjana Juric, Head of Service for combating irregularities and fraud, Ministry of Finance, Croatia; Philippe de Koster, Director FIU Belgium; Prof. Dr. Katalin Ligeti, University of Luxembourg; Prof. Dr. Ralf Poscher, Director at the Max Planck Institute for the Study of Crime, Security and Law, Freiburg, Germany; Lorenzo Salazar, Deputy Prosecutor General to the Court of Appeal of Naples, Italy; Prof. Rosaria Sicurella, University of Catania, Italy
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

ISSN: 1862-6947

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 the Managing Editor:

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