eucrim
2022 / 1
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

The Prevention of and Fight against Money Laundering – New Trends
La prévention et la lutte contre le blanchiment d'argent – Nouvelles tendances
Prävention und Bekämpfung der Geldwäsche – neue Trends

2022 / 1 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*

European Union

Council of Europe

Articles

The Prevention of and Fight against Money Laundering – New Trends

* 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,

The past year was again a challenging one for Europe and the world, due to the persisting COVID-19 pandemic. 2021 was also marked by one of the largest global money laundering scandals in recent history – the "Pandora Papers." It demonstrated the growing scale of the money laundering threat and the persistence of launderers in abusing the international financial system to hide their illicit proceeds.

We are facing a combination of older and newer money laundering methods – both requiring coordinated action from governments in Europe and around the world. Traditional money laundering uses offshore jurisdictions while concealing the true ownership of assets behind several layers of "shell" companies. Specialised "gatekeepers," e.g., lawyers, accountants, and other service providers often help launderers set up such companies, trusts, etc. The "Pandora papers," like the "Panama Papers" five years ago, showed that "gatekeepers" can be complicit in large-scale, transnational money laundering schemes involving corrupt politicians and high-net worth individuals seeking to evade taxes. This is the reason why MONEYVAL has been focusing on such professions and working with the FATF to enhance their regulatory regime. In 2021, we achieved an important change in the international FATF standard to regulate the transnational operations of "gatekeepers." This change will oblige certain professions to establish group-wide anti-money laundering programmes and pave the way for tighter supervisory cooperation among governments. These measures will be challenging to implement, since supervisory cooperation in this area did not exist before. However, governments must mobilise their efforts in order to finally curb the money laundering abuses we have witnessed in recent years.

One money laundering trend is related to the emerging virtual assets sector – the increasing global use of cryptocurrencies – and other components of the rapidly evolving ecosystem of "decentralised finance". This alternative system removes the traditional forms of control that banks and institutions have on financial flows and services. In most cases, the components of one single crypto-business are spread across multiple countries. It creates enforcement and supervisory challenges for governments, due to rapidly evolving tech infrastructure, the cross-border nature of financial services, and difficulties in determining which national jurisdiction is responsible for their oversight. Supervisory cooperation in this field is in its very nascent stages and is not yet keeping pace with the rapid evolution of technology.

The difficulties with supervision of both "gatekeepers" and virtual assets can only be overcome by using innovative supervisory methods. Necessitated by the challenges of the pandemic, MONEYVAL has just completed a typologies study looking into supervisory practice in times of crisis and under challenging external circumstances, which is sure to help us improve supervision.

Elżbieta Franków-Jaśkiewicz

It is well known that money launderers have been abusing cryptocurrencies from their inception over a decade ago, initially to transfer and conceal proceeds from drug trafficking. Nowadays, their methods are becoming increasingly sophisticated and take place on a larger scale. Today, virtual assets are abused to launder proceeds from fraud, corruption, and tax evasion. The larger virtual assets are seeing heavy market manipulation, which is a major predicate offense for money laundering. These challenges require a clear and comprehensive response, and MONEYVAL is taking extensive measures in this area. MONEYVAL's evaluations and follow-up processes are now closely looking into the regulatory framework for virtual assets in member states, and a 2022 typologies study will be solely dedicated to cryptocurrency money laundering trends.

It is clear that Europe continues to face significant money laundering challenges. However, enhanced cooperation and commitment between our law enforcement agencies, supervisory authorities, financial intelligence units, and the private sector as well as effective cross-border cooperation will give us the capacity to tackle existing and new threats.

Ms Elżbieta Franków-Jaśkiewicz, Chair of MONEYVAL

In Memoriam Mireille Delmas-Marty

Prof. Dr. Dr. h.c. mult Ulrich Sieber, Editor in Chief

On 12 February 2022, Professor Mireille Delmas-Marty passed away at the age of 80 in Saint-Germain-Laval, France. We have lost a brilliant criminal lawyer and philosopher, a passionate advocate of human rights and legal humanism, and the discerning architect of European criminal law.

I

Mireille Delmas-Marty, who studied law and held a doctorate in philosophy, taught at the universities of Lille II, Paris XI, and Paris I Panthéon-Sorbonne, and she was a member of the Institut Universitaire de France. She was – undoubtedly the rare crowning achievement of an academic career in France – appointed to the Collège de France, where she held the chair in Comparative Legal Studies and Internationalization of Law, and was elected a member of the Academy of Moral and Political Sciences. The French Republic appointed her Grand Officier de la Légion d'honneur and awarded her the Ordre national du Mérite. Eight honorary doctorates from renowned international universities reflect the high regard in which Mireille Delmas-Marty was also held abroad. She received, among other distinctions, the first Hans Heinrich Jescheck Prize conferred by the International Association of Penal Law and the Max Planck Institute for Foreign and International Criminal Law as well as the Beccaria Medal awarded by the International Society of Social Defence and Humane Criminal Policy.

II

The scientific work of this distinguished scholar is characterised by clear goals and values. A major focus of her research was the *development of law in the globalised world*. Mireille Delmas-Marty perceptively analysed the fundamental tensions confronting law in this area: Even though each community has its own "compass" with its own regulations and rites, the ubiquitous spread of globalisation is simultaneously having a profound effect on legal systems. In view of these conflicting currents and the uncertainties associated with them, Delmas-Marty did not aim to find a "new North Pole" on the "bussole des possibilités", her "compass of possibilities", but rather to reconcile the pluralism of the different cultures with the universalism of globalisation. She did not wish to create a new, general "global law" but instead to show "how to move from the great chaos of deregulated globalism to a kind of 'ordered pluralism' that brings differences together without suppressing them." She was not concerned with the unification of law but rather with approximation, creating "a common legal area ... that preserve[s] diversity." According to Delmas-Marty, "differences must remain, but they must become compatible." In the context of this "harmonisation imparfaite," a "marge d'appréciation" remains for the states by which to prevent universal imperialism. This margin of appreciation is both at the core of her legal policy demands and also analysed in her fundamental comparative research on "Les chemins de l'harmonisation pénal".

III

Mireille Delmas-Marty's decisive compass for the law of the globalised world is based on *human rights and a new, pluralistic and open legal humanism.* In her quest to find a new "common law of humanity", she suggested adapting the law to the challenges of globalisation in a forward-looking and often visionary manner. Using the climate crisis and the Covid-19 pandemic as examples, she made it clear that classical state sovereignty must shift towards a "souveraineté solidaire" in benefit of the "solidary protection of global common goods". Similarly, she called for greater accountability on the part of non-state actors, especially business entities. In order to prevent the collapse of modern society, Delmas-Marty advocated the further development of human rights-based, universal guidelines with regard to terrorism, financial crises, and migration. She drew attention to the increasing interdependencies emerging in the globalised world, the lacking predictability of problems, and the forces of fear and risk steering society today. As a committed representative of freedom rights, she cautioned against a "society of fear" instead of a "community of destiny" and yet retained an optimistic world view: "In the end, the unpredictable calls for thinking ... with confidence in the human adventure ... It is not the fear of perishing but the ambition to live that has thrown human beings onto the roads of the earth, the sea and the sky." In order to solve problems, "la puissance des forces imaginantes du droit" ("the power of the imaginative forces of law") played a key role in shaping her compass of politi-

cal possibilities. With her "humanisme juridique", the grande dame of European criminal law was undeniably also a source of hope for a new, better world.

IV

In addition to the fundamental issues mentioned above, Mireille Delmas-Marty's numerous and frequently translated publications cover a *wide range of related topics*.

- In *European criminal law*, she gained renown especially through the "Corpus Juris" project: She headed the working group, which presented comprehensive substantive and procedural guiding principles for the protection of the EU's financial interests in 1997. The "Corpus Juris" also developed the idea of the European Public Prosecutor's Office for the European legal space, which has since become reality. In addition to exploring these issues in a multi-volume implementation study, there is a vast body of work on central questions of European law to her credit, including the six-volume study on criminal sanctions in Europe, which she co-edited. She also published important academic treatises in collaboration with her peers in the field of international (public) criminal law. Most recently, Delmas-Marty had been particularly active in international, environmental, and climate protection – always with her finger on the pulse of time.
- In the field of *comparative criminal law*, she published a wealth of impressive publications, together with foreign colleagues, such as "Les grands systèmes de politique criminelle", "European Criminal Procedures", "The criminal process and human rights", and "Modèles et mouvements de politique criminelle". These fundamental works, as well as her detailed studies on the comparison of French and Chinese law (especially her analyses of white-collar crime, human dignity, and cloning) document that she was an eminent comparative law scholar and, moreover, that she was keenly aware of the differences in norms in the pluralistic world from direct experience.
- In *French law*, Delmas-Marty wrote the leading work on economic criminal law: a two-volume book on "Droit pénal des affaires", now in its 4th edition. She also pushed for a new conception of a modern human rights-based code of criminal procedure. Other publications in which she championed civil liberties concerned the vagueness in criminal law, the French law on terrorism, and the "droit pénal de la dangerosité". She pleaded against the "disaster-narrative, inspired by fear, ... in the face of the 'risks of risks', from prevention to precaution and even prediction."

V

Mireille Delmas-Marty was also strongly committed to the *practical implementation* of her research findings. Early in her professional career, she already dealt with legal policy issues as a member of the national commissions for the revision of the French Constitution (1992), the reform of the Criminal Code (1981), and the reform of the law of criminal procedure (1988). She was a member and president of the Supervisory Committee of the European Anti-Fraud Office (OLAF). For many years, she also served on the board responsible for the EU Rule of Law Programme in China and advised the Prosecutor of the International Criminal Court. In all these and many other important cooperation projects, she has left an enduring legacy. She was highly respected, and her expertise was avidly sought in practice – above and beyond criminal law. The authoritative researcher impressed all those who knew her with her brilliant mind and her steadfast values but especially also in person with her grace, her willingness to help, and her unfailing kindness.

VI

Mireille Delmas-Marty was unquestionably the visionary cultivator of a humanist criminal law in an ordered pluralism of the globalised world. Her work reflects the true embodiment of the *conscience of the global criminal justice system*. After her passing, the philosopher Edgar Morin expressed this aptly with the words "Quelle grande et belle conscience qui s'en va.": What a great and beautiful conscience that is departing. Indeed, one of the most brilliant legal scholars of the 21st century and an inspiring role model has left us. Her outstanding analyses and keen visions, her legal humanism, and her exceptional works, however, will remain and continue to show us the way towards a better, peaceful, and solidary world.

Chère Mireille, merci beaucoup!

News

Actualités / Kurzmeldungen*

European Union

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

Foundations

Fundamental Rights

EP Resolution on EU's 2021 Annual Report on Human Rights and Democracy

On 17 February 2022, the European Parliament (EP) adopted a resolution on the EU's 2021 annual report on human rights and democracy. The EP recommended that the EU Special Representative for Human Rights (EUSR) devote special attention to the countries/topics addressed in Parliament's monthly urgency resolutions on human rights abuses and to any human rights violations, notably those committed under authoritarian regimes. It also encouraged the EUSR to pursue diplomatic efforts to enhance the EU's support for international humanitarian law and international justice. The EP strongly condemned all attacks against the mandate holders of UN special procedures and against the independence and impartiality of their mandates. It pointed out that state sovereignty cannot be used as a pretext to avoid human rights monitoring by the international community and also underlined the need for adequate funding of all UN human rights bodies.

The EP reiterated its strong support for the International Criminal Court (ICC) as the only international institution able to prosecute some of the world's most heinous crimes and able to deliver justice for the victims. In order to uphold the independence and impartiality of the ICC, the EP called on the EU and the Member States to provide adequate financial support to enable the ICC to carry out its tasks. It strongly condemns any attacks on the staff or independence of the ICC.

MEPs also urgently called for the creation of an EU-wide scheme to issue short-term visas for the temporary relocation of human rights defenders and strongly condemned the killing of human rights defenders around the world. Justice and accountability for these attacks at the highest level of decision-making is demanded.

The EP further spoke out against the use of SLAPPs, i.e. the rise of legal harassment and restrictive legislation as a means of silencing critical voices (→eucrim 4/2021, 223–224 and eucrim 3/2021, 161). One such form of harassment involves strategic lawsuits against public participation and even the criminalisation of defamation online and offline, which is used to scare off journalists, whistleblowers, and human rights defenders. The Parliament also voiced concerns about the restriction of academic freedom and an increase in the censorship and imprisonment of scholars worldwide.

Ultimately, the EP remarked that artificial intelligence must be developed, deployed, and used under meaningful human supervision, in full transparency and ensuring accountability and non-discrimination, in particular to avoid both bias in automated decisions and data protection violations. (AP)

Proposal for Directive on Corporate Sustainability Due Diligence

On 23 February 2022, the European Commission adopted a proposal for a Directive on corporate sustainability due diligence. With this proposal, the Commission aims to foster sustainable and responsible corporate behaviour throughout global value chains. The proposal is the response of the Commission to a call from the European Parliament in March 2021, and from the Council on 3 December 2020, to submit a legislative proposal on mandatory value chain due diligence.

* Unless stated otherwise, the news items in the following sections (both EU and CoE) cover the period 1 January–31 March 2022. Have a look at the eucrim website (https://eucrim.eu), too, where all news items have been published beforehand.

According to the proposal, companies will be required to identify and prevent, end, or mitigate the adverse impacts of their activities on human rights and on the environment. The following EU companies and sectors will be subject to the new due diligence rules:

- up 1: All EU limited liability companies of substantial size and economic power (500+ employees and €150 million+ in net turnover worldwide).
- Group 2: Other limited liability companies operating in defined high-impact sectors (>250 employees and a net turnover of €40 million or more worldwide).

The rules will start to apply two years later for companies from group 2 than for group 1. The companies from both groups will need to demonstrate compliance with the new proposal as follows :

- Integrate due diligence into corporate strategies;
- Identify actual or potential adverse human rights and environmental impacts;
- Prevent or mitigate potential impacts;
- Bring to an end or minimise actual impacts;
- Establish and maintain a complaints procedure;
- Monitor the effectiveness of due diligence policy and measures;
- Publicly communicate on due diligence.

Regarding corporate sustainability due diligence, the proposal provides for two tracks of enforcement: First, Member States will be obliged to designate an administrative authority which will supervise and impose effective, proportionate and dissuasive sanctions, including fines and compliance orders. At European level, the Commission will set up a European Network of Supervisory Authorities that will bring together representatives of the national bodies to ensure a coordinated approach. Second, Member States must ensure civil liability, so that victims get compensation for damages resulting from the failure to comply with the obligations of the new rules. (AP)

Poland: Rule-of-Law Developments January – March 2022

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 4/2021, 200–201.

- 19 January 2022: The Commission sends a demand for payment of €69 million to the Polish government, as Poland has not yet given in to the dispute over the operation of the controversial Disciplinary Chamber of the Polish Supreme Court. Poland has so far refused to comply with a payment order by the CJEU's Vice-President of 27 October 2021 (→eucrim 4/2021, 200) that fined Poland for not having implemented interim measures to cease the exercise of the new competences by the Disciplinary Chamber. The Polish government now has 45 days to comply with the payment request. In the last resort, the money could be offset against EU funding for Poland.
- 3 February 2022: The European Court of Human Rights (ECtHR) confirmed previous judgments that the Polish Supreme Court does not meet the standards of the right to a fair trial enshrined in Art. 6 ECHR. In the case at issue (Application no. 1469/29, Advance Pharma SP.Z O.O v Poland), a Polish company instituted claims for damages in tort against the Polish State; its appeal was dismissed by the Civil Chamber of the Polish Supreme Court at last instance. The ECtHR shared the view that the Civil Chamber of the Polish Supreme Court is not a "tribunal established by law" and lacks impartiality and independence within the meaning of Art. 6(1) ECHR. The violation mainly resulted from the amendments to Polish legislation which deprived the Polish judiciary of the right to elect judicial members of the National Council of the Judiciary (NCJ) and enabled the executive and the legislature to interfere directly or indirectly in the judicial appointment procedure. This systematically compromised the legitimacy of a court composed of the judges appointed in that way. The ECtHR criticizes the Polish State for disregarding rulings by the CJEU and Polish courts that declared the judicial reform not in conformity with EU and national law. The judges in Strasbourg call on the Polish State to stop the perpetuation of the systemic dysfunction and to take rapid action to remedy the situation in accordance with Art. 46 ECHR.
- 8 February 2022: The ECtHR orders Poland, by way of an interim measure, to ensure that the Disciplinary Chamber of the Polish Supreme Court does not decide on the waiver of immunity of a Polish judge until the final determination of the complaint by the ECtHR. In the case at issue (Application no. 6904/22, *Wróbel v Poland*), the complainant is a Supreme Court judge and co-author of a Supreme Court resolution denying the Disciplinary Chamber to be an "independent tribunal established by law". Charges are pending against him before the Disciplinary Chamber for "criminal negligence in relation to a judicial decision given in a criminal case", which could result in the waiver of his immunity. According to the ECtHR, these proceedings must now be suspended until the ECtHR has decided on the merits of the case, i.e. whether the complainant's right to a fair trial under Art. 6 ECHR was respected. The ECtHR issues such interim measures only exceptionally if the complainant would otherwise face a real risk of irreparable harm.
- 9 February 2022: The General Court confirms that the CJEU's case law on the rule of law in European Arrest Warrant cases applies, by analogy, in competition cases. In the case at issue (Case T-791/19, *Sped-Pro v Commission*), a Polish company complained before the European Commission about the abuse of a dominant position on the market for rail freight transport services by the PKP Cargo S.A., a company controlled by the Polish State. The Commission rejected the complaint and pointed to the Polish competition authority which would be best placed to examine the case. Ac-

cording to the General Court states the Commission must ensure that the fundamental right to a fair trial before an independent tribunal enshrined in Art. 47(2) of the Charter of Fundamental Rights is, like in the area of freedom, security and justice, also guaranteed in competition cases that affect the effective application of Arts. 101 and 102 TFEU. National courts must be in a position to review the legality of decisions of the national competition authorities and to directly apply Arts. 101 and 102 TFEU. If the Commission examines the European interests it must assess, as a first step, whether there is a real risk of a breach of the right connected with a lack of independence of the courts of the Member State in question, on account of systemic or generalised deficiencies in that State, and, as a second step, whether the person concerned actually runs a real risk, having regard to the particular circumstances of the case. In the present case, the judges in Luxembourg blamed the Commission for having failed to examine adduced evidence that the complaining Polish company runs a real risk of a breach of its rights because its case will not appropriately be treated by the Polish authorities and courts.

■ 16 February 2022: Following the CJEU's judgment that upheld the validity of the Regulation on the conditionality mechanism (→spotlight under "Protection of Financial Interests"), EP President *Roberta Metsola* commented: "The European Parliament now expects the Commission to apply the conditionality mechanism swiftly. Conditionality of EU funds linked to respect of the rule of law is non-negotiable for the European Parliament."

■ 21–23 February 2022: An EP delegation travels to Poland to assess respect of EU values. MEPs meet with government officials, national authorities, the judiciary, civil society and media organisations. The mission collects information with a focus on the separation of powers, the independence of the judiciary, the situation of fundamental and minority rights, and the effects of the Polish Constitutional Tribunal's standpoint on the primacy of EU law.

■ 22 February 2022: The General Affairs Council holds its fifth hearing on the rule of law in Poland under the Article 7(1) TEU procedure. The hearing is a precondition for the Council to determine that there is a clear risk of a serious breach by a Member State of the values referred to in Art. 2 TEU. The purpose of the hearings is to provide the Council with an updated picture of the situation and to help integrate developments since the last hearing on 22 June 2021. Commission Vice-President *Vera Jourová* stressed in the meeting that the Commission maintains its rule-of-law concerns particularly due to the activity of the Polish Constitutional Tribunal, the National Council of the Judiciary and the disciplinary regime for judges and prosecutors in Poland.

■ 10 March 2022: The Polish Constitutional Tribunal confirms a motion by Polish Prosecutor General and Minister of Justice *Zbigniew Ziobro* and argues that certain ways the ECtHR had interpreted Art. 6(1) ECHR in cases against the judicial reform in Poland are unconstitutional. In essence, the Constitutional Tribunal stated that the ECtHR and national courts "are not authorized to assess the organisation of the judiciary, the competence of courts, and the law defining the organisation, procedure and method of election of members of the (Polish) National Council of the Judiciary". In addition, the Constitutional Tribunal stressed that the Polish constitution does not allow the ECtHR or national courts "to disregard constitutional provisions, laws and judgments of the Polish Constitutional Tribunal". Last but not least, the Constitutional Tribunal believes that Art. 6(1) ECHR "cannot include a judge's subjective right to hold an administrative position within the structure of the common judiciary in the Polish legal system". The motion and the judgment (case K 7/21) is seen as a reaction to ECtHR judgments of November 2021, in which the judges in Strasbourg confirmed the irregularity of Polish judges' appointments and a violation of the right to an independent and impartial tribunal established by law (cases *Dolińska-Ficek, Ozimek v Poland* →eucrim 4/2021, 201). Critics to the motion said that the Polish Minister of Justice wanted to receive green light from the Constitutional Tribunal in order not to comply with the ECtHR rulings. The judgment of the Constitutional Tribunal resembles its controversial judgment of 7 October 2021, in which it declared the interpretation of Arts. 1 and 19 of the EU Treaty as interpreted by the CJEU inconsistent with the Polish Constitution (case K 3/21 →eucrim 3/2021, 137).

■ 13 March 2022: 27 former judges of the Polish Constitutional Tribunal protest against the judgment of the same court of 10 March 2022. They state that the judgment in question "is another scandalous example of jurisprudence violating the Constitution" and stressed that "[t]his deepens the crisis of the constitutional state, including in particular the principle of a democratic state of law and the principle of separation of powers, and causes growing isolation of Poland in Europe." The former judges also draw attention to the worrying circumstances in which the judgment was released.

■ 22 March 2022: The CJEU (Grand Chamber) declared inadmissible an action for preliminary ruling in which the Polish Supreme Court (chamber for labour and social insurance law) asked whether EU law confers on it the power to decide that a court president did not have a valid judge's mandate to initiate disciplinary proceedings against another judge before a disciplinary court due to the Polish reforms of the judiciary (Case C-508/19). The judges in Luxembourg stated that the questions referred are hypothetical because the referring court lacked jurisdiction as the main issue – the legal relationship of the judge who initiated disciplinary proceedings – is a

public law question, not a civil one. It is up to the judge who faced disciplinary proceedings to object before the disciplinary court that said dispute is not determined by an independent and impartial tribunal previously established by law as previously ruled by the CJEU. In its opinion of 15 April 2021, Advocate General *Tanchev* believed that the reference for preliminary ruling is admissible and that the referring court can establish a flagrant breach of the judge's appointment.

■ 25 March 2022: 94 judges of the Polish Supreme Court call on the Polish parliamentarians to fully implement the judgments of the ECtHR and the CJEU and to liquidate the main source of problems with the rule of law, namely the new National Council for Judiciary (neo-NCJ). The appeal comes along the start of debates on several bills that are to address the Polish disciplinary chambers and the reform of the Supreme Court.

■ 31 March 2022: OKO.press reports that Acting First President of the Supreme Court *Małgorzata Manowska* and the Disciplinary Commissioner of the Supreme Court are intensifying repression against Polish judges who want to examine the legality of the appointment of a neo-judge by the new, politicised National Council for Judiciary (neo-NCJ) and to apply the judgments of the ECtHR and CJEU which found the appointments to the NCJ incompatible with European rules.

■ 31 March 2022: A new bill launched by the governing PIS party on the "protection of the population" sparks criticism since it would enable the government to restrict constitutional freedoms without parliamentary control and to remove undesirable mayors at the local level. (TW)

CJEU again Finds Romanian Judicial System Flawed

In the dispute between the Court of Justice of the EU and national constitutional courts over the distribution of competences, the CJEU, sitting in for the Grand Chamber, blamed the Romanian justice system. In its judgment of 22 February 2022 (Case C-430/21), the CJEU clarified its line of argumentation regarding judicial independence (enshrined in the second subparagraph of Art. 19(1) TEU) read together with the primacy of EU law. Accordingly, EU law precludes a national rule under which national courts have no jurisdiction to examine the conformity with EU law of national legislation which has been held to be constitutional by a judgment of the constitutional court of the Member State.

➤ *Background of the case*

In the case at issue, a Romanian court considered it necessary to examine, in the context of an appeal procedure, whether the national legislation establishing a specialised section within the public prosecutor's office for the investigation of criminal offences committed within the judiciary was compatible with Union law. The CJEU already ruled in 2021 (Cases C-83/19, C-127/19 et al.) that the establishment of the specialised section was contrary to EU law if its establishment is not justified by objective and verifiable requirements relating to the sound administration of justice and is not accompanied by specific guarantees. Following this judgment, the Romanian Constitutional Court confirmed, however, its previous findings that provisions on the aforesaid creation of the specialised section were constitutional. It argued that, whilst Art. 148(2) of the Romanian Constitution provides for the primacy of EU law over contrary provisions of national law, that principle cannot remove or negate national constitutional identity. Furthermore, the Romanian Constitutional Court stated that an ordinary court was not competent to examine the conformity with Union law of a national regulation that had been declared compatible with the constitutional provision requiring respect for the principle of the primacy of Union law.

In those circumstances, the Romanian appeal court was in a conflict and therefore referred the matter to the CJEU asking whether it must comply with the case law of the Constitutional Court or has jurisdiction to examine the conformity with EU law of the legislation establishing the specialised section within the prosecution office. In addition, the referring court pointed out that, according to the current rules, national judges are put at risk of exposure to disciplinary proceedings and penalties, if they examine the conformity with EU law of a provision of national law that the Romanian constitutional court has found to be constitutional.

➤ *Ruling of the CJEU*

The judges in Luxembourg found such national rules and practices incompatible with EU law and emphasised *inter alia*:

■ The necessity for national courts to fully apply any provision of EU law having direct effect ensures equality of Member States and expresses the principle of sincere cooperation (Art. 4(3) TEU). This allows national courts to disapply contrary national provisions of their own motion;

■ Preventing national courts from assessing the compatibility of national provisions with EU law and the requirement to comply with judgments of the constitutional court would preclude the full effectiveness of the rules of EU law;

■ Such national rules or practice would undermine the system of cooperation between the CJEU and national courts since ordinary courts would be deterred from ruling on the dispute by submitting preliminary ruling requests.

In addition, the judges in Luxembourg argued that only the CJEU itself, as the highest EU court, is competent to interpret common Union law in a binding manner. A national constitutional court cannot itself decide that the CJEU had exceeded its jurisdiction with a judgement and therefore reject to give effect to a preliminary ruling judgement. A national constitutional court may not disapply an EU provision even if it considers the national identity of the Mem-

ber State threatened. It would then be up to the CJEU to decide.

Ultimately, EU law (Art. 2 and 19(1) TEU) preclude that national judges may incur disciplinary sanctions if they ignore a decision of the constitutional court and appeal to the CJEU.

➤ *Put in focus*

The CJEU's Grand Chamber already took a similar decision in December 2021 (→eucrim 4/2021, 214). In the context of the effective protection of the EU's financial interests, the judges in Luxembourg clarified that EU law takes precedence over the national constitution. At that time, the CJEU ruled that Romanian courts can disapply decisions of the Constitutional Court in certain cases. (TW)

Area of Freedom, Security and Justice

Impact of War in Ukraine on Justice and Home Affairs

The Russian invasion of Ukraine that started on 24 February 2022 has also several repercussion on the justice and home affairs policy of the EU. An extraordinary meeting of the Justice and Home Affairs Council took place on 27 February 2022 at which ministers decided to activate the EU Integrated Political Crisis Response (IPCR) arrangements. The IPCR is a mechanism by which the Council Presidency coordinates the political response to major cross sectoral and complex crises. The extraordinary meeting addressed aspects of humanitarian support, the reception of refugees, management of the EU's external borders, visa measures, and the anticipation of hybrid threats.

On 3 March 2022, the Council issued a statement in which EU home affairs ministers unanimously agreed on the establishment of a temporary protection mechanism in response to the influx of displaced persons from Ukraine. This entailed activation of Directive 2001/55/EC of 20 July 2001 on minimum standards for providing temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof. EU Member States are now able to offer people fleeing the conflict in Ukraine a protected status similar to that of refugees – in any EU country – for a renewable period of one year.

On 4 March 2022, The ministers for justice agreed that the processing of requests for extradition and mutual legal assistance in criminal matters submitted by Russia and Belarus should be suspended. However, this should be without prejudice to an examination on a case-by-case basis. Furthermore, sanctions imposed on Russian oligarchs should be implemented effectively; if necessary anti-money laundering efforts must be increased. Commissioner *Didier Reynders* announced the establishment of a task force in this context.

There was also a strong consensus that Member States want to support the investigations of the International Criminal Court (ICC). The measures taken by some Member States to gather evidence on war crimes were welcomed. Eurojust was encouraged to fully exercise its coordinating role and to collaborate with the ICC prosecutor.

On 7 March, the JHA Council published a joint statement together with the Justice and Home Affairs Agencies, in which the agencies offered, as a matter of urgency, their assistance to EU institutions and Member States within the margins of their respective expertise. (CR/TW)

Assessment of the Current State of Data Innovation

On 2 February 2022, the Joint Research Centre (J.R.C.), the European Commission's science and knowledge service, published its Science for Policy report on Data Innovation in Demography, Migration and Human Mobility. This report is not intended to present a policy position of the European Commission but rather to present the evidence-based output that scientifically supports the European policy-making process in the areas of demography, migration, and human mobility.

The report acknowledged that, although the availability of data has become central to policymakers when making informed policy decisions, data innovation has also led to new challenges with regard to ethics, privacy, data governance models, and data quality. The purpose of the report was to assess the current state of data innovation in the scientific literature.

The report highlighted three main findings:

- *Advantages of using innovative data*: Innovative data is composed of data derived from an individual's digital footprint, from sensor-enabled objects, and/or can be inferred using algorithms. The study found that, in comparison to traditional data, innovative data have a greater geographic and temporal granularity, (near-)real time availability, and allow extensive coverage, which makes more immediate international comparisons possible. After reviewing the scientific literature, the report concluded that mixed methodologies were increasingly being used, namely integrating traditional data with innovative data in order to study demographic and migration phenomena. The report also showed that there is a discrepancy with regard to the definitions of population, migration, and human mobility between the studies that were based on innovative data and those studies adopted for official statistics;
- *Greatest potential of data innovation*: The study showed that data innovation was best used in the domains of "situational awareness, nowcasting and response" and of "prediction and forecasting," as it has the potential to provide (almost) real-time, accurate, and detailed information on demographic trends and/or public opinions;
- *Facilitation of data innovation transition*: In order to fully unleash the po-

tential of non-traditional data, there needs to be a transition from a phase of exploratory use of innovative data to a phase of systematic use of innovative data for official statistics and policy-making. The report stressed that legislation is undoubtedly a *sine qua non* condition of data innovation transition. Legislation has different roles to play in this transition: It should regulate the access to data held by the private sector in a way that guarantees the individual's fundamental rights and the interests of the private sector. It should also explore how to allow national statistical offices to collect, analyse, and publish data from non-traditional data sources. Alongside a favourable regulatory framework for data innovation transition, more investments need to be made that are aimed at fostering collaboration between data owners and the private and public research sectors. (AP)

Security Union

Commission Proposes New Regulations to Improve Cybersecurity and Information Security of EU Administration

On 22 March 2022, the Commission made two new proposals to improve cybersecurity and information security in EU institutions, bodies, offices, and agencies: a Cybersecurity Regulation and an Information Security Regulation.

➤ *Cybersecurity Regulation*

With this regulation, the Commission wishes to establish common cybersecurity measures across the EU's institutions, bodies, offices, and agencies. The regulation is in line with the Commission's priorities to make Europe fit for the digital age. The measures include the following:

- Strengthening the mandate of the Computer Emergency Response Team (CERT-EU) and providing the resources needed to fulfil it;
- Modernising the existing CERT-EU legal framework in order to take into account the altered and increased digitisation of EU institutions, bodies, and agencies as well as the changing cybersecurity threat landscape;
- Changing the name of the computer centre from "Computer Emergency Response Team" to "Cybersecurity Centre". The abbreviation "CERT-EU" will be kept for name recognition purposes;
- Setting up a new inter-institutional Cybersecurity Board to drive and monitor implementation of the regulation and to steer CERT-EU.

All EU institutions, bodies, offices, and agencies are called on to do as follows:

- Put in place a framework for governance, risk management, and control in the area of cybersecurity;
- Implement a baseline of cybersecurity measures addressing the identified risks;
- Conduct regular maturity assessments;
- Put in place a plan for improving their cybersecurity.

➤ *Information Security Regulation*

The regulation on information security is part of the EU Security Union Strategy adopted by the Commission on 24 July 2020 (→eucrim 2/2020, 71–72), which is intended to bring the EU's added value to national efforts in the area of security. The goal is to provide a stable foundation for the secure exchange of information across EU institutions, bodies, offices, and agencies and with the Member States. With this proposal, the Commission aims to achieve the following:

- To set up an inter-institutional Information Security Coordination Group that will foster cooperation across all EU institutions, bodies, offices, and agencies;
- To establish a common approach to information categorisation, based on the level of confidentiality;
- To modernise information security policies, fully including digital transformation and remote work.

The proposals are an outcome of the EU's strategy to bolster resilience of its administration against cyber and information threats. (AP)

Schengen

Council Adopts General Approach on New Schengen Evaluation Procedure

On 3 March 2022, the Justice and Home Affairs Council agreed on a general approach regarding the reform of the specific Schengen evaluation and monitoring mechanism (for the Commission proposal →eucrim 2/2021, 76). The new rules will speed up and simplify the evaluation procedures, and strengthen the political and operational steering. The new Regulation will repeal the legal framework of 2013. Enhancements will particularly be done in the following areas:

- New strategic focus of the mechanism, which will include multiannual evaluation programmes and better targeted unannounced and thematic evaluations;
- Simpler and faster evaluation and monitoring procedures – here, the new Regulation will streamline the evaluation documents, provide an escalation mechanism in the event of lack of progress, and introduce a fast-track procedure for the identification of and response to serious deficiencies;
- Improved pooling of expertise, including the involvement of EU agencies, such as Frontex and Europol;
- Enhanced role of the Council.

The Council decided to consult the European Parliament for an opinion on the proposed new Regulation. The Regulation itself will then only be adopted by the Council. (TW)

French Council Presidency Wants Better Use of SIS against Terrorists

At the beginning of its Council Presidency, France initiated discussion of whether the post-hit procedure in the Schengen Information System (SIS) for alerts related to terrorism should be improved. Under the current law, only

two EU Member States and Europol exchange information on terrorists. If an individual was registered in the SIS by the "issuing" Member State and was located or detected by the "checking" Member State" only these two states exchange further information. In addition, the issuing State is required to send this "hit" to Europol.

The French Council Presidency now proposed that all Member States having previously volunteered receive alerts on certain terrorists and are mandatorily and automatically informed of the hits. According to the proposal, this will concern alerts on Islamist terrorists released from prison and linked to Syrian-Iraqi networks, Europeans who have left for the Syrian-Iraqi conflict zone and try to come back to Europe, and foreign terrorist fighters.

The proposal aims to better detect threatening individuals who particularly entered the European territory in migratory flows and then freely move within the Schengen area benefitting from the absence of internal border checks. The French Council Presidency expects a more precise monitoring if all volunteering EU Member States are informed of these individuals once detected. In addition, the improved information flow should enable Member States to issue restrictive or surveillance measures more rapidly and to use the date for future investigations. In a document circulated on 21 February 2022, the French Council Presidency further explained its proposal including ideas on how the new procedure could be technically implemented in the SIS. The document also sets out that legislation on the SIS must be revised and starts discussion on the operational need for a reform. The outcome of the discussions in the Council working groups might lead to respective Council conclusions at the end of the French Presidency.

Civil society organisations criticised the initiative for significantly increasing the amount of personal data that will be exchanged between national authorities. The proposal did also not contain an impact assessment thus it is feared that "it will lead to magnifying and expanding the preventive surveillance powers of the volunteering member states that will receive notifications of hits and it will provide the justification for extensive data collection, for example mass retention of telecommunication metadata under the banner of national security". Ultimately, critics point out that changes to the category of terrorist alerts may put other individuals, e.g. "political activists", into consideration of national security authorities. (TW)

Legislation

Commission Proposes Declaration on European Digital Rights and Principles

spot light

On 26 February 2022, the Commission proposed a Declaration on digital rights and principles for a human-centred digital transformation. The Commission builds upon previous Council initiatives such as the Tallinn Declaration on eGovernment, the Berlin Declaration on Digital Society and Value-based Digital Government, and the Lisbon Declaration – Digital Democracy with a Purpose. The proposal was shaped through consultation and exchange with citizens and interested parties.

The adoption should take the form of a joint solemn declaration to be signed by the European Parliament, the Council, and the Commission. In doing so, the Commission wishes to define a set of principles for a human-centred digital transformation and make sure that the values of the Union and the rights and freedoms of individuals as guaranteed by Union law are respected and reinforced both offline and online.

The Commission has recognised that digital technologies and emerging technological breakthroughs are transforming every aspect of our lives and have a great impact on how the economy and society are organised. These developments, which have become accelerated in the wake of COVID-19, have also increased the digital divide across the EU – the divide between well-connected urban areas and rural/remote territories and the one between those who can benefit from an accessible and secure digital environment and those who cannot. It is therefore vital that all actors (such as administrations, research and education institutions) ensure inclusiveness, so that everyone can benefit from digital transformation. However, these new digital technologies and digital data can also entail undesirable risks that can have far-reaching effects for citizens, democratic values, and security. In line with the 2030 Digital Compass (→eucrim 1/2021, 8–9), the Commission would like to define a set of principles that will serve as guidance for a sustainable, human-centric, and value-based digital transformation.

The Commission therefore proposed that the EU should be committed to the following:

- To put people at the centre of the digital transformation by strengthening the democratic framework for a digital transformation that benefits everyone and by taking the necessary measures to ensure that the values of the Union and the rights of individuals are respected both online and offline;
- To strengthen solidarity and inclusion by making sure that technological solutions respect people's rights, enable the exercise of these rights, and promote inclusion, thus making sure that digital transformation leaves no one behind, and by developing adequate frameworks so that all market actors benefit from the digital transformation;
- To ensure access to excellent connectivity for everyone;
- To ensure the right to digital education and skills for everyone by promoting and supporting efforts to equip all education and training institutions with digital connectivity, infrastructure, and tools;

- To ensure that everyone is able to "disconnect" and benefit from safeguards for a better work-life balance in the digital environment;
- To ensure that all Europeans are offered an accessible, secure, and trusted digital identity that enables access to a broad range of online services;
- To empower European citizens to benefit from the advantages of artificial intelligence (AI) while protecting them against risks that the use of AI might entail;
- To ensure a safe, secure, and fair online environment in which fundamental rights are protected;
- To continue safeguarding fundamental rights online, notably the freedom of expression and information;
- To take measures to tackle all forms of illegal content and to create an online environment in which people are protected against disinformation and other forms of harmful content;
- To ensure the possibility to easily move personal data between different digital services;
- To support the development and use of sustainable digital technologies that have a minimal environmental and social impact. (AP)

AIDA Adopts Report on Artificial Intelligence in a Digital Age

On 22 March 2022, the Parliament's Special Committee on Artificial Intelligence in a Digital Age (AIDA) adopted a report on artificial intelligence (AI) which emphasised that the digital transition in the EU must be human-centric and compatible with the Charter of Fundamental Rights of the EU. The report includes a motion for a EP resolution on AI in the digital age, which will be put to a vote by the plenary in May. The report is the main output of the AIDA Committee's work, which it took up in September 2020. AIDA was tasked with exploring the impact of AI on the EU economy and its different sectors, with analysing the AI approach of third countries, and with charting the road ahead.

In the report, the MEPs caution that the EU has fallen behind in the global race for tech leadership. This might result in a risk for standards that need to be developed elsewhere in the future, often by non-democratic actors.

In order to focus on the enormous potential that AI offers to human beings, AIDA identified policy options that could unlock AI's potential in the areas of health, the environment, and climate change. They also see the potential for AI – combined with the necessary support infrastructure, education, and training – to increase capital and labour productivity, innovation, sustainable growth, and enhance job creation.

The report stressed that the use of AI poses crucial ethical and legal questions, especially with regard to military research and technological developments of AI, which can be transformed into lethal, autonomous weapon systems. Another point of concern is the possible use of AI for mass surveillance and other unlawful interference, such as the profiling of citizens in order to rank them and restrict their freedom of movement, which in turn poses a threat to fundamental rights – in particular the rights to privacy and data protection. (AP)

Assessment of EU Legislation in the Digital Field

On 31 January 2022, the EP published a scientific study on the "Identification and assessment of existing and draft EU legislation in the digital field". The study was conducted at the request of the special committee on Artificial Intelligence in a Digital Age (AIDA). It provides an overview of digital legislation and possible regulatory gaps, as there has been a phase of great legislative production in the last few years and an even faster pace of development in digital technologies and their applications. The study aims to:

- Give a systematic overview of existing and upcoming digital regulations and directives;
- Analyse and systematise the interplay between the most important legislative acts and their coherence;
- Identify regulatory gaps.

In so doing, the study has identified gaps in the European Commission proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) adopted on 21 April 2021 (→eucrim 2/2021, 77).

According to the study, the Artificial Intelligence Act (AI Act) did not take into account social scoring, biometric identification systems, and AI systems for military-purposes. The study also criticised that it is not clear to what extent high risks have been consistently identified throughout all relevant regulations and whether the high-risk category should lead to the application of strict liability regimes in any event. The interplay between the AI Act – as the core component of the AI regulatory framework – and other legal acts might hinder the development of a flawless regulatory framework for AI in the EU. This is especially true with regard to the interplay between the AI Act and the General Data Protection Regulation (GDPR), because more clarity in the AI Act with regard to the processing of personal data is needed.

Furthermore, the interplay between the liability exemption – under the e-Commerce Directive – and the intensive use of algorithmic decision-making in content moderation, notice and removal, complaint-handling, and conflict solving is creating additional points of friction. This raises the question of whether the poor performance of algorithmic voluntary measures in failing to detect (illegal/inappropriate) content should be interpreted as explicit operator knowledge, triggering a duty to react and a resultant liability.

The study also stressed problems regarding the interplay between AI and cybersecurity, as AI might aggravate cybersecurity risks by rendering cyberattacks more easily targeted and more destructive, on one hand. On the other

hand, AI systems may also enhance the effectiveness of preventive measures against cyber-attacks serving as a shield against cybersecurity breaches.

Ultimately, there are potential problems regarding the implementation of the Open Data Directive in relation to the proposed Data Governance Act, in the Database Directive, in the P2B Regulation, in the Digital Services Act (DSA), and in the Digital Markets Act (DMA). Overall, coherence and simplicity has been overlooked in the building of a European regulatory system for the digital domain, according to the authors of the study. (AP)

45 Civil Society Organisations Call for Prohibition of Predictive and Profiling AI Systems in Law Enforcement and Criminal Justice

45 Civil society organisations issued a call for the prohibition of AI predictive and profiling AI systems in law enforcement and criminal justice in the Artificial Intelligence Act (→eucrim 2/2021, 70). They see a danger in the use of these systems that will lead to the following problems:

- An increase in discrimination, surveillance, and over-policing: The organisations claim that the law enforcement and criminal justice data used to create, train and operate AI systems is often biased and will therefore reinforce the discrimination, surveillance, and over-policing of racialised people, communities, and geographic areas.
- A violation of the right to liberty, the right to a fair trial, and the presumption of innocence: Predictive profiling and risk assessment AI systems in the area of law enforcement and criminal justice will lead to the profiling of individuals and groups as criminals before they have even carried out the alleged acts for which they are being profiled. Serious criminal justice and civil outcomes and punishments, including deprivations of liberty may therefore occur even before the individuals or groups have acted criminally.
- A violation of the right to an effective remedy, risks of intransparency, and problems with accountability: Individuals affected by decisions made by these systems should be made aware of their use and informed about clear and effective routes of criminal procedure by which to challenge the use of these systems.

Against this background, the civil society organisations therefore stressed that such systems must be included as a "prohibited AI practice" in Article 5 of the planned Artificial Intelligence Act. (AP)

EP Adopted Position on Digital Services Act

On 20 January 2022, the European Parliament adopted its position regarding the proposal for a regulation on a Single Market For Digital Services (Digital Services Act). The EP amended several dispositions of the Commission proposal (→eucrim 4/2020, 273). The DSA primarily concerns online intermediaries and platforms (e.g. online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms). The aim is to create a safer digital space in which the fundamental rights of users are protected.

In order to achieve the objective of ensuring a safe and trusted online environment, the concept of "illegal content" should be understood broadly – it should underpin the general idea that what is illegal offline should also be illegal online.

Among the major amendments by the EP:

- In order to assist Member States and service providers, the Commission should provide guidelines that clarify any potential conflicts between the conditions and obligations laid down in legal acts (referred to in this Regulation), explaining which legal act should prevail;
- Providers of intermediary services should make efforts to ensure that, where automated tools are used for content moderation, the technology can be sufficiently relied on to limit (to the maximum extent possible) the rate of error, namely when information is wrongly considered to be illegal content;
- Member States should not prevent providers of intermediary services from providing end-to-end encrypted services;
- In accordance with the principle of data minimisation and in order to prevent unauthorised disclosure, identity theft, and other forms of abuse of personal data, Member States should not impose a general obligation on providers of intermediary services to limit the anonymous use of their services;
- Member States should ensure full implementation of the Union's legal framework on confidentiality of communications and online privacy as well as on the protection of natural persons with regard to the processing of personal data enshrined in Directive (EU) 2016/680;
- Providers of intermediary services should also be required to designate a single point of contact for recipients of services, which allows rapid, direct, and efficient communication – in particular by easily accessible means using telephone numbers, email addresses, electronic contact forms, chatbots, and instant messaging;
- Online platforms should ensure that recipients can understand how recommender systems impact the way information is displayed and how this can influence how information is presented. They should clearly indicate the parameters for such recommender systems in an easily comprehensible manner in order to ensure that the recipients understand how information is prioritised for them;
- Online platforms should not use personal data for commercial purposes related to direct marketing, profiling, and behaviourally targeted advertising of minors. Targeting individuals on the basis of special categories of data, especially targeting vulnerable groups, should not be permitted;
- The Commission should ensure that it is independent and impartial in its deci-

sion-making with regard to both digital services coordinators and providers of services defined in this Regulation.
- The Commission should carry out a general evaluation of the DSA Regulation and submit a report to? the European Parliament, the Council, and the European Economic and Social Committee. (AP)

Institutions

European Parliament

New EP President Elected

On 18 January 2022, Ms *Roberta Metsola* was elected new President of the European Parliament, having served as its Vice-President since November 2020. Of the three candidates, Ms *Metsola* received an absolute majority of 458 votes out of 690 cast in the remote secret vote. She follows in the footsteps of the former President of the European Parliament, *David Sassoli*, who passed away on 11 January 2022.

Roberta Metsola is a member of the Group of the European People's Party (EPP). She was born in 1979 in Malta and has been an MEP since 2013. She is the youngest EP President ever elected and the third woman to hold this post. In her opening address, Ms *Metsola* underlined the need to fight against anti-EU narratives, disinformation and misinformation, nationalism, authoritarianism, protectionism, and isolationism. (CR)

Three New Committees at EP

Following a proposal by the Conference of Presidents, the European Parliament set up three new committees:
- A committee of inquiry to look into the Pegasus spyware;
- A special committee to look into malicious foreign interference;
- A special committee to look into the European response to the COVID-19 pandemic.

Starting from their constitutive meetings, the three new committees will have twelve months to compile their recommendations.

The "Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware" will look into the use of the surveillance software by Member States and investigate whether the spyware was used for political purposes. The Parliament wants to investigate alleged breaches or maladministration in the implementation of EU law. It will consist of 38 members. Its term of office is twelve months and can be extended twice by three-month periods (see Rule 208 of the Rules of Procedure of the EP).

The "Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation II" will have a look at existing and planned EU legislation in order to find loopholes that could be exploited by third countries for malicious purposes. It will continue the work of its homonymous predecessor. The committee will have 33 members. Its term of office is limited to 12 months, which can be extended by Parliament before the period expires (see Rule 207 of the Rules of Procedure of the EP).

The Special Committee on "COVID-19 pandemic: lessons learned and recommendations for the future" will take a close look into the European response to the pandemic in the areas of health, democracy and fundamental rights, economy and society, and the EU's global relationships. The committee will consist of 38 members. Its term of office is limited to 12 months, which can be extended by Parliament before the period expires (see said Rule 207 of the Rules of Procedure of the EP). (AP)

European Court of Justice (ECJ)

CJEU: Judicial Statistics 2021

On 2 March 2022, the Court of Justice of the EU published its judicial statistics for the year 2021.

Looking at the number of cases brought before the Court of Justice and the General Court, the year 2021 once again confirmed the upward trend with 1.720 new cases brought before the two courts compared to 1.683 cases in 2018, 1.905 cases in 2019, and 1.584 cases in 2020 during the peak of the pandemic.

Regarding the number of references for preliminary ruling to the CJEU in 2021, a total of 587 references were filed from the courts of the Member States. The subjects addressed in these references included for example:
- Rule of law;
- The environment;
- Protection of personal data;
- Social protection;
- The fight against violence against women
- Consumer protection.

In this context, the Court points out how much its activities closely reflect contemporary concerns and challenges. (CR)

General Court: New Judges Appointed

On 13 January 2022, the Court of Justice of the EU held a formal sitting on the occasion of the entry into office of three new Judges of the General Court of the EU: Mr *Damjan Kukovec*, Ms *Suzanne Kingston*, and Mr *Ioannis Dimitrakopoulos*.

Mr *Kukovec* started his professional career as a lawyer at the Slovenian Court of Appeal, followed by positions at the Special Court for Sierra Leone, the Constitutional Court of Slovenia, and as a lawyer at the Court of Justice of the EU and for the Legal Service of the European Commission. He has also pursued an academic career, at the same time carrying out various teaching activities in EU law. He was appointed judge at the General Court for the period from 22 December 2021 to 31 August 2025.

Ms *Kingston* has practised law at the Bar of Ireland as a barrister and as senior counsel and also taught law as a professor at University College Dublin and at several other universities. She succeeds

Mr *Anthony Collins* and was also appointed to the Court for the period from 22 December 2021 to 31 August 2025.

Mr *Dimitrakopoulos* succeeds Mr *Dimitrios Gratsias* as judge at the General Court of the EU for the period from 22 December 2021 to 31 August 2022. Before joining the Court, he served as assistant judge to the Greek Supreme Special Court and as Alternate Chairman of the Board of Appeal of the European Chemicals Agency. Since 2010, he has also been professor at the Greek National School of Judicial Officers. (CR)

OLAF

Arrangement between OLAF and EUIPO

On 1 March 2022, a new Service-Level Agreement between OLAF and the European Union Intellectual Property Office (EUIPO) became effective. The agreement aims at increasing cooperation when it comes to crimes against intellectual property. It foresees, *inter alia*, the development of an IT tool, which will make it easier to share and analyse data related to counterfeiting cases at EU level. Furthermore, the agreement includes provisions on joint trainings and the support of operations organised by OLAF and involving the authorities of the EU Member States.

OLAF Director-General *Ville Itälä* and EUIPO Executive Director *Christian Archambeau* stressed that tackling IP crimes is one of the EU's priorities in fighting organised crime. The agreement will serve to make this fight more effective and to prevent gangs and criminals from benefiting from counterfeiting. (TW)

Cooperation Arrangement between OLAF and Hungarian Prosecutor General

On 11 February 2022, OLAF reported that it signed a cooperation arrangement with the Office of the Prosecutor General of Hungary. The arrangement lays down practical modalities for closer cooperation in order to protect EU funds from potential fraud in the country. This is also important since Hungary does not participate in the scheme of enhanced cooperation regarding the EPPO. The arrangement with OLAF includes *inter alia*:

- Information sharing between OLAF and the Hungarian Prosecutor General on specific investigations;
- Operational assistance;
- Shared training opportunities and technical assistance.

According to Hungarian Prosecutor General *Péter Polt*, the arrangement formalised the already excellent cooperation between OLAF and the Prosecution Service of Hungary, which has so far been fulfilled by the parties on the basis of common interests and objectives. Hungary is also the only country of the non-participating states to the EPPO that concluded a working arrangement with the new Office (→eucrim 1/2021, 14). (TW)

Illegal Tobacco Trade Operations in 2021

On 23 February 2022, OLAF informed of the results of its operations against tobacco smuggling in 2021 (for the results in 2020 →eucrim 1/2021, 14). In 2021, world-wide operations involving OLAF were able to seize over 430 million illicit cigarettes in total. The majority (253 million) was seized outside the EU borders preventing the illicit cigarettes from flooding the EU market. OLAF also helped take down illegal production sites across the EU, which amounted to the seizure of 91 million cigarettes. 372 tonnes of raw tobacco were confiscated. Contraband or counterfeit waterpipe tobacco remains a trend that has increasingly affected OLAF's activities. OLAF was able to identify suspicious consignments for over 60 tonnes of waterpipe tobacco.

OLAF Director-General *Ville Itälä* said: "These seizures have saved EU Member States roughly 90 million euro in lost revenue, and we have helped target the criminal gangs that are behind this illegal business. Smugglers deploy various tricks and schemes (for example declaring at customs almost 10 million illicit cigarettes as suitcases) and they have adapted their business model to the pandemic, and to tougher controls at the EU's borders." (TW)

OLAF Support in Dismantling Fake Medicine Network

On 16 February 2022, a joint operation between OLAF and the Polish police dismantled a gang that dealt with counterfeit medical products, such as medicine to treat erectile dysfunction, anabolic substances and growth hormones. The value of the seized goods is estimated at almost €9 million. OLAF assisted by retracing the smuggling route of the goods which stemmed from Asia and were imported to Poland via other EU countries. (TW)

OLAF JIT Uncovers Tomato Swindle

On 19 January 2022, OLAF reported on the results of a joint investigation team (JIT) involving OLAF, the Romanian National Anticorruption Directorate (DNA) and the Prosecution Office of the Italian commune of Enna. The investigations revealed practices of a criminal group that defrauded EU agricultural funds worth €850,000. The group established shell companies in Romania and submitted false leases and invoices, thus receiving EU funds for farms allegedly producing tomatoes, even though farming never took place. After having received the funds, the money was transferred to Italy where it was quickly withdrawn in order to finance other criminal activities. 9 persons must now stand trial in Romania on charges of fraud. The European Commission's Directorate-General for Agriculture and Rural Development is recommended to recover the full funding amount of €850,000.

Eurojust also supported the investigations. The Agency assisted in the exchange of information and coordination of parallel investigations, in particular as regards the issuance and enforcement of freezing orders on the assets of the suspects and their companies. (TW)

European Public Prosecutor's Office

EPPO's First Annual Report

spot light

On 24 March 2022, the EPPO published its first annual report, which gives account of the office's operational activities from 1 June to 31 December 2021. The report provides an overview of and statistical data on the operational activities of the central office in Luxembourg and all 22 participating Member States. It also outlines typologies identified in EPPO cases and recovery actions regarding the proceeds of criminal activity. Other sections report on the following:

- Activity of the College;
- Activity of the Permanent Chambers;
- Activity of the Operations and College Support Unit;
- Case Management System and IT;
- Human resources and staff development;
- Financial resources and their management;
- Transparency and relations with the general public and the press;
- Activity of the Legal Service;
- Data protection;
- Relations of the EPPO with its partners.

➤ *Key figures*

In the first seven months of operation, the EPPO processed 2832 crime reports. 576 investigations were opened, and 515 investigations were active by the end of the year. The estimated damage to the EU's budget was around €5.4 billion, whereby €147 million were seized upon request by the EPPO. 122 staff members work in the central office in Luxembourg. 95 European Delegated Prosecutors have been appointed, who work in 35 EPPO offices in the 22 participating Member States.

➤ *Typologies of criminal offences*

The most frequent types of crime affecting the EU's financial interests that were identified in the 515 active cases were as follows:

- The majority of EPPO investigations (31.8%) concern suspected non-procurement fraud in conjunction with the use/presentation of false, incorrect, or incomplete statements/documents, as a result of which funds or assets from the Union budget or budgets managed by the Union were illegally retained;
- 17.6% of the EPPO investigations concern the most serious forms of VAT fraud (in particular carousel fraud), VAT fraud through missing traders, and VAT fraud committed within a criminal organisation. These fraud schemes occur mostly in the automotive, electronic device, and textile sectors and usually involve a number of companies acting in several countries, either as buffer traders, brokers, or as missing traders;
- 13.4% of the EPPO investigations concern non-VAT revenue fraud (in particular customs and anti-dumping duties fraud). This type of fraud is found across nearly all types of merchandise, e.g. tobacco, electronics, bicycles, spare parts, etc;
- Procurement expenditure fraud makes up 11.2% of the investigations. Usually, offences are committed by using/presenting false, incorrect, or incomplete statements/documents. Forgery is a common inextricably linked offence. Procurement fraud occurs mainly in connection with construction, waste and wastewater infrastructure subsidies, technology (green waste, recycling), and human resources development programmes;
- 4% of the EPPO cases involve the active or passive corruption of public officials.

➤ *EPPO's added value*

The report highlighted that the cooperation regime – as established in the EPPO Regulation – has proven to be very efficient and speedy (compared to the traditional mutual legal assistance arrangements).

➤ *Cooperation with non-participating EU and third countries*

Regarding cooperation with the five non-participating EU Member States, cooperation with Poland proved particularly cumbersome. Of these non-participating states, Poland is responsible for causing the most EPPO cases (23 of a total of 48 cases involving non-participating states), but the country systematically hindered the EPPO in its efforts to obtain evidence located in Poland (→page 22). A working arrangement with the National Prosecutor's Office of Poland failed.

The EPPO succeeded, however, in concluding a working arrangement with the office of the Prosecutor General of Hungary in April 2021 (→eucrim 1/2021, 14). The country caused 17 EPPO cases in 2021.

Working arrangements with Irish and Danish authorities could not be concluded in 2021, but negotiations are to be resumed in 2022. These countries had a low rate of causing EPPO cases in 2021.

Cooperation with Sweden was smooth. The relevant EU acts on judicial cooperation in criminal matters contributed to this positive state of affairs.

Regarding third countries, the EPPO initiated negotiations with the aim of concluding working arrangements with the relevant authorities of the United States of America and of Ukraine (for the arrangement concluded with Ukraine in the meantime →following news item). China is the third country that has contributed to most of the EPPO cases (13 out of 45 cases involving third countries).

➤ *Cooperation with European and international institutions/bodies*

To allow for a quicker exchange of information, the EPPO signed several working arrangements at the European level. It has working arrangements with the European Commission, Eurojust, Europol, OLAF, the European Court of Auditors, the European Investment Bank, and the European Investment Fund (→previous eucrim issues).

Regarding cooperation at the international level, the EPPO joined the Camden Asset Recovery Inter-agency Network (CARIN) as an observer. It also initiated discussions with the Fi-

nancial Action Task Force (FATF) and the OECD Working Group on Bribery in International Business Transactions (WGB), with the aim of participating in theses bodies.

➤ *Comments by the European Chief Prosecutor*

Upon presenting the report, European Chief Prosecutor *Laura Kövesi* said: "European cannot mean weak! The EPPO is a very powerful tool for protecting expenditures as well as revenues of the EU budget by means of criminal law. 20 years after the Euro zone, we have created the EPPO zone. Embedded in the national judiciaries of the 22 participating Member States, the EPPO is in the first line of defence of the rule of law in the EU. The first 7 months of our operations made at least one thing clear: if we are hindered in the exercise of our competence, the protection of the EU budget is at stake." (TW)

Working Arrangement Between EPPO and Prosecutor General's Office of Ukraine

On 18 March 2022, European Chief Prosecutor *Laura Kövesi* and Ukrainian Prosecutor General *Iryna Venediktova* signed a working arrangement. *Kövesi* conveyed the support of the EPPO College to the Ukrainian colleagues, praising the strength and courage of Ukraine especially in the times of war. Furthermore, *Kövesi* assured that the EPPO will support its Ukrainian counterparts on their way to the EU with all available means.

The working arrangement sets out the framework for judicial cooperation in criminal matters and the exchange of information between the parties.

Regarding operational cooperation, the parties undertake to widely cooperate on the gathering of evidence and the freezing of assets in accordance with the existing international legal framework, in particular the 1959 CoE MLA Convention and its protocols and the 2005 CoE Anti-Money Laundering Convention. The setting up of joint investigation teams in cases that fall under the EPPO's competence is also agreed on. The Ukraine recognizes extradition requests that are submitted by the competent authorities of the Member State of the handling European Delegated Prosecutor.

Other provisions of the working arrangement include:

- The exchange of strategic information;
- The secondment of liaison officers to the EPPO;
- EPPO contact points in Ukraine;
- High-level meetings, training sessions and other events;
- Technical support provided by the EPPO;
- Means and channels of communication;
- Protection of personal data, data security and liability. (TW)

Working Arrangement Between EPPO and Italian Customs Authority

On 23 February 2022, a working arrangement between the EPPO and the Italian excise, customs and monopolies agency (Agenzia delle Dogane e dei Monopoli, ADM) entered into force. The arrangement provides for closer cooperation and communication in the fight against crimes that affect the EU's financial interests. A key element is that the EPPO offices in Italy can instruct a special unit at the ADM to carry out investigations or to support ongoing investigations. (TW)

Working Arrangement Between EPPO and Greek Audit Authority

On 10 February 2022, a working arrangement between the EPPO and the Hellenic National Transparency Authority (NTA) was concluded. The arrangement provides for an improved structured framework for cooperation in accordance with the existing applicable legislation. The arrangement sets out *inter alia*:

- The modalities and channels for information exchange;
- Scientific and technical support by the NTA to EPPO investigations;
- Priority treatment of EPPO cases by the NTA;
- Exchange of information on individual cases and of strategic information;
- Data protection rules.

The NTA is an independent audit authority that was created in 2019 through an administrative reform in Greece. It is mandated to enhance transparency, integrity and accountability of Greek state bodies and to prevent and detect cases of fraud and corruption in the administration. (TW)

Working Arrangement Between EPPO and General Council of the Judiciary of Spain

On 2 February 2022, the EPPO signed a working agreement with the Spanish General Council of the Judiciary. The arrangement will enable the EPPO to use the so-called "Judicial Neutral Point" – a service network with applications and databases of the General Council. The arrangement also details the cooperation in the fight against crimes that affect the EU's financial interests. The EPPO made several commitments to use the network correctly and confidentially.

The working arrangement is valid for four years, renewable, and will be reviewed at least once a year by a Mixed Monitoring Commission. (TW)

EPPO's Struggle with Slovenia in Next Round

On 27 January 2022, European Chief Prosecutor *Laura Kövesi* voiced concerns over planned amendments to the statute of limitations in the Slovenian criminal law. The comments came when the Slovenian Prosecutor-General visited *Kövesi* and her two deputies. The EPPO is worried about the hampering of proper fraud investigations should the reform be adopted. Accordingly, Slovenian prosecutors would drastically have less time to investigate and many cases may be immediately and definitely closed. *Kövesi* said that the new legisla-

tion would represent a de facto amnesty for many cases of fraud against the EU budget in Slovenia and it will also have a negative impact on Slovenia's cooperation with other Member States since assisting measures may not be performed in Slovenia.

Kövesi also informed the public that she addressed a letter to the European Commission in line with Recital 16 of Regulation (EU) 2020/2092 of 16 December 2020 on a general regime of conditionality for the protection of the Union Budget. The Regulation is the basis for the EU to interrupt, reduce, terminate or suspend payments from the EU budget to an EU country which does not guarantee the sound financial management of the EU's financial interests due to breaches of the principles of the rule-of-law (→eucrim 3/2020, 174–176). Recital 16 of that Regulation provides that the Commission must identify breaches of rule-of-law principles thorough a qualitative assessment, which should take into account relevant information from available sources and recognised institutions, including, *inter alia*, the EPPO. For a similar letter by the EPPO on the situation in Poland →page 22.

The European Chief Prosecutor was already in struggle with Slovenia last year since the Slovenian government persistently obstructed the nomination of the Slovenian Delegated Prosecutors, so that the office was paralysed to effectively conduct fraud investigations in Slovenia when it started in June 2021. In November 2021, the EPPO College could finally appoint the Slovenian colleagues, although the Slovenian government upheld some reservations (→eucrim 4/2021, 209–210). (TW)

EPPO: Operational Activities – Reports from January to March 2022

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 January/February/March 2022 include the following:

■ On 22 March 2022, at the request of the Bulgarian European Delegated Prosecutor, Bulgarian law enforcement carried out searches and seizures against Bulgarian companies for suspected subsidy fraud. The companies allegedly belong to an organised crime group that unlawfully received EU funds for the support of small and medium-sized companies. Construction materials worth €6 million, documents and hardware were seized.

■ On 16 March 2022, officers of the Lithuanian Special Investigation Service conducted searches in Klaipėda (Lithuania) and other locations in Lithuania against an organised group that allegedly illegally obtained EU funds (estimated to €200,000). The operation was conducted in the context of investigations led by the Lithuanian European Delegated Prosecutor against suspects for abuse of office, fraud and forgery of documents. EU money was received for construction works.

■ On 15 March 2022, the Guardia di Finanza of Savona (Italy) executed an order by the pre-trial judge as applied for by the EPPO and seized several luxury vehicles worth €750,000. Investigations revealed that a man who formally resides in a South American country but permanently lives in Italy did not pay customs duties and VAT (approximately €250,000) when he introduced luxury and vintage cars and motorcycles into Italian territory. The investigations are led by the EPPO office in Torino for aggravated smuggling.

■ On 15 March 2022, the EPPO saw the first operation in Portugal. The operation dubbed "Operation Europe" targeted smuggling of textiles and shoes from China to Europe through Portuguese territory. Led by two Portuguese and one investigative judge, several law enforcement officers conducted searches in private residences, lawyers' offices, accounting firms and customs brokers in several locations in Portugal. The damage of the fraud scheme to the EU's financial interests amounts to at least €600,000.

■ On 9 March 2022, an operation in cooperation with the Carabinieri Command for Agri-Food Protection of Messina (Italy) resulted in the seizure of €200,000. The case concerns non-procurement fraud by two farmers who deceived about the size and ownership of the lands, and thus unlawfully received EU money.

■ On 23 February 2022, the EPPO in Rome, in cooperation with the Rome Customs Office, seized nearly €350,000 in cash from an Italian company. The company evaded customs duties and VAT on the import of surgical masks from China. It was revealed that a portion of the masks were branched off against the EU's duty free rules and that the masks did not comply with EU safety regulations, putting all users of the masks and patients at risk.

■ On 15 February 2022, the EPPO cracked down on an organized criminal group in Bulgaria. With the support of the Bulgarian police four suspects were detained and their homes and offices searched. The defendants are suspected of having made false statements in order to obtain funds from the European Social Fund and under a measure to overcome the economic consequences of the COVID-19 pandemic. The exact damage is still being determined.

■ On 7 February 2022, the Italian Customs and Monopolies Agency seized €130,000 from a Sicilian company as part of an EPPO investigation. This company imported e-bikes from China and falsely declared the country of origin as Malaysia, thus evading anti-dumping duties. The case was initiated by a report from OLAF. The defendant was charged with aggravated smuggling by the EPPO office in Palermo.

■ On 4 February 2022, the EPPO informed of the results of investigations carried out by the Hanover Customs Investigation Office under the supervision of the EPPO office in Hamburg, Germany. The investigations have been conducted since 2021 and targeted a scheme of commercial and organised tax

evasion with the import of luxury cars by several international criminal groups in Germany and Estonia. With the support of customs offices in Germany, 26 searches were carried out and vehicles with a total value of €3.6 million were seized. Investigations and actions also involved the EPPO offices in Estonia and Latvia; investigators from the Hanover Customs Investigation Office took part in search activities in Estonia. The estimated total tax loss amounts to at least €5 million.

- On 3 February 2022, the EPPO office in Naples (Italy) led an operation against four companies and two individuals. The case involves the import of disassembled e-bikes from China and Turkey and the false declaration of these parts instead of complete e-bikes. As a result, the fraudsters paid less VAT. The fraudsters also used shell companies in Turkey in order to hide the true origin from China, thus evading anti-dumping rules. The damage amounts to around €13 million.
- On 24 January 2022, a tobacco smuggling case investigated by the EPPO led to the first indictment in Lithuania. The case involved two Lithuanian customs officials who assisted two citizens of the Republic of Belarus in smuggling cigarettes into EU territory. The estimated damage to the EU and Lithuanian budget is believed to be close to €10 million.
- On 20 January 2022, the first indictment of an EPPO case in Bulgaria was tried by the Specialised Criminal Court in Sofia. The case relates to bribery, in which a general expert working for the Bulgarian State Fund Agriculture (SFA), received money from a farmer, in order to accelerate the payments of EU subsidies. The verdict is expected in the coming months.
- On 11 January 2022, the Slovak office of the EPPO conducted an operation against four companies suspected of VAT and customs fraud in Slovakia and the Czech Republic. The total damage is estimated at around €48 million. The fraud scheme was based on undervaluation of import goods and the circumvention of customs duties. (TW)

Europol

EDPS Orders Erasure of Personal Data Not Categorised by Europol

On 3 January 2022, the European Data Protection Supervisor (EDPS) issued an order against Europol to delete data concerning individuals with no established link to a criminal activity. The "Decision on the retention by Europol of datasets lacking Data Subject Categorisation ('DSC')" follows from the EDPS' long-standing inquiry into large datasets stored at Europol without the needed categorisation as foreseen in the Europol Regulation (→eucrim 3/2020, 169–170).

Large datasets lacking DSC refer to datasets which, because of their characteristics and notably their size, do not undergo the data classification process and extraction of data categories as provided for in the Europol Regulation and its Annexes. This is a recurrent problem since Europol receives complex and large datasets for analysis where a pre-categorisation of individuals linked to a criminal activity (e.g. suspects, witnesses, contact persons to criminals, etc.) is hardly possible. However, under the current rules, Europol is not allowed to keep data on individuals who have no established link to crime or criminal activity for a prolonged period of time.

With a view to contributions of categories of personal data and data subjects within the meaning of Art. 18(5) of Regulation 2016/794, the EDPS orders Europol the following:

- To proceed with data subject categorisation for each contribution within six months of the date of receipt;
- To erase datasets lacking DSC after expiry of the six-month period;
- Not to perform data processing operations with the personal data (other than that strictly necessary to proceed with such categorisation) before the DSC is completed;
- To proceed with DSC regarding existing datasets within twelve months;
- To notify (where applicable) the third parties, to whom datasets lacking DSC have been disclosed, of the erasure of the datasets;
- To provide quarterly implementation reports over the next twelve months.

Following this decision, on 11 January 2022, Europol published a statement claiming that the decision will impact Europol's ability to analyse complex and large datasets at the request of EU law enforcement. Europol's work frequently entails a period longer than six months, as does the police investigations it supports. Hence, the Agency will assess possible consequences and any negative impact of the decision and seek the guidance of its Management Board.

A possible revision of the current Europol Regulation (→eucrim 4/2020, 279) will tackle the problem and probably prolong the time limits for Europol to assess large-scale datasets. (CR)

Open Letter: Reconsideration of Europol's Data Processing Capacities

Following the EDPS decision on the retention of datasets lacking data subject categorisation (→news item above), a consortium of 23 civil society organisations from across Europe and beyond sent an open letter to European policymakers on 26 January 2021. The letter urges them to seriously reconsider expansion of Europol's data processing capacities as foreseen under the draft provisions of the proposal amending the Europol Regulation (→eucrim 2/2021, 83). (CR)

Cooperation with Russia Suspended

On 17 March 2022, as a consequence of the situation in Ukraine, the Europol Management Board decided to suspend any cooperation with Russia. This decision also affects the strategic agreement concluded in November 2003. Furthermore, Europol will continue to work at all levels to support the EU Member States impacted by the conflict. (CR)

Annual Report of the European Migrant Smuggling Centre

On 23 February 2022, the European Migrant Smuggling Centre (EMSC) at Europol published its sixth annual report for the year 2021. The report once again confirms migrant smuggling and trafficking in human beings (THB) as being among the most serious criminal threats facing the EU.

According to the report, migrant smuggling activities along most of the routes to and within the EU increased in 2021. Although migrant smuggling relies on a variety of means of transport, leaders of smuggling networks can increasingly coordinate their criminal operations remotely, thereby making lucrative profits.

As for THB, the report states that the crime is being increasingly digitalized, involving THB processes such as recruitment, contacts, the advertising of services conducted online, and remote coordination of operations. In addition, victims are very often identified and recruited via the Internet's ability to reach a broad audience. Sexual exploitation remains the most frequently reported form of THB in the EU, but labour exploitation is also increasingly being reported.

Lastly, the report points to the Europol Monitoring Team Report – a weekly intelligence picture on migrant smuggling and trafficking in human beings, which issued its 500th edition in 2021. (CR)

Europol Report on Criminal Use of Cryptocurrencies

At the end of January 2022, Europol published a new report containing an overview of the illicit use of cryptocurrencies. The report provides core definitions, case examples, and details of the challenges authorities face in combating the illicit use of such digital currencies.

In its findings, the report clears up a series of myths surrounding the criminal use of cryptocurrencies. It disproves the idea that cryptocurrencies have become the payment method of choice for criminals, as the overall number and value of cryptocurrency transactions related to criminal activities still make up only a small amount of the criminal economy when compared to cash and other forms of transaction.

In addition, the report clarifies that the criminal use of cryptocurrencies is not limited to cybercrime activities but also relates to all types of crime that require the transmission of a monetary value, including fraud and drug trafficking. It reveals that illicit funds increasingly pass through a multi-step process involving financial entities, many of which are new and not yet part of standardised, regulated financial and payment markets and thus do not flow straight from wallet to wallet, as often assumed.

Lastly, the report underlines that cryptocurrencies are not anonymous but rather offer law enforcement access to substantially more information than cases involving cash, given that every single transaction is logged onto a blockchain. Most blockchains are publicly available, making transactions traceable. (CR)

Eurojust

Eurojust Annual Report 2021 – 20 Years of Criminal Justice Assistance

At the beginning of March 2022, Eurojust published its Annual Report for the year 2021. Last year, Eurojust celebrated its 20th anniversary and, for the first time in its history, the Agency supported more than 10,000 cases in one single year.

On its 20th anniversary, Eurojust had 337 post-holders, including 26 National Members, assisted by 57 deputies and assistants seconded from the judicial authorities of the Member States. Ten Liaison Prosecutors from countries outside the EU are also posted at Eurojust. The Agency holds international/cooperation agreements with 13 third countries and is actively connected with over 60 jurisdictions worldwide. It also actively cooperates with main actors in the EU criminal justice area, such as Europol, OLAF, eu-LISA, FRA, and EUIPO. Additionally, in 2021, Eurojust signed a working agreement with the EPPO. The Agency's budget amounted to €53.3 million in 2021.

The total number of cases supported by the Agency increased 15% compared to the previous year, totalling 10,105 cross-border criminal investigations in the past year. 4808 cases were new cases and 5297 were ongoing cases from previous years. As in previous years, the majority of new cases concerned swindling and fraud (1453), money laundering (648), and drug trafficking (869).

Eurojust provided operational guidance on the application of EU judicial cooperation instruments, in particular with regard to the European Arrest Warrant (480 cases), the European Investigation Order (4.262 cases), freezing and confiscation, and conflicts of jurisdiction. It also provided expert advice on securing (electronic) evidence across EU borders.

In 2021, Eurojust supported 72 new Joint Investigation Teams (JITs) and provided €1.16 million in funding for 104 active JITs. The Agency extended its financial support to also cover the costs of specialist expertise, low-value equipment (hardware, software), and travel/accommodation/interpreting for victims and witnesses.

Eurojust's governance and agency management included the adoption and implementation of an anti-fraud strategy 2021–2024. Other activities included the approval of the Agency's Multi-Annual Strategy for 2022–2024. (CR)

New Liaison Prosecutor for the UK

In the first week of March 2022, Mr *Christopher Williams* took up his position as Liaison Prosecutor for the United Kingdom at Eurojust. Prior to joining Eurojust, Mr *Williams* served as prosecutor and head of unit within the Specialist Fraud Division of the Crown Prosecution Service (CPS), handling major international fraud cases. Mr *Williams* succeeds Ms *Samantha Shallow*,

who was previously National Member and later Liaison Prosecutor for the UK at Eurojust. (CR)

First JIT with the EPPO

In February 2022, Eurojust supported the setting up of a Joint Investigation Team (JIT) with the European Public Prosecutor's Office (EPPO) for the first time. As the case concerned cross-border VAT or carousel fraud of over €10 million, it fell under the competence of the newly created EPPO. The JIT was signed by Sweden and the French EDP at the EPPO. Given that Sweden, whose authorities were involved in the investigation, is not participating in the EPPO, the Swedish authorities had asked Eurojust to assist the investigations between them and the EPPO. (CR)

Support by Eurojust Leads to Conviction for Crimes against Humanity

For the first time worldwide, a high-ranking Syrian official was convicted for crimes against humanity. The former member of the Syrian intelligence services was sentenced to life imprisonment for the deaths – as a result of torture and inhumane imprisonment conditions – of 27 members of the regime's opposition. The judgement, handed down by the German Higher Regional Court of Koblenz on 13 January 2022, marked the final step in a joint investigation set up in 2018 between Germany and France and supported by Eurojust and its Genocide Network. (CR)

Frontex

New Register of Public Documents Launched

At the beginning of March 2022, Frontex launched a new register of public documents. This is an online library containing public documents produced by the Agency since its foundation in 2004. The register can be searched by categories and subcategories, language, publication dates and keywords. It is also a gateway to other Frontex registers, such as the Public Access to Documents (PAD), the data protection register, or the transparency register as well as to Frontex calls, tenders and vacancies. The register fulfills obligations under Regulation (EU) 1049/2001 and follows the good practices agreed in response to an inquiry by the European Ombudsman (→eucrim 1/2021, 18–19). (CR)

Support to Member States Neighbouring Ukraine

At the beginning of March 2022, Frontex started assisting Romanian authorities in processing the number of people crossing the border from Ukraine in the wake of the Russian war and perform other border control-related tasks, if needed. Hence, the Agency sent about 150 officers, 45 patrol cars, and other equipment to Romania's border with Moldova and Ukraine. The operation follows a request from the Romanian authorities. Furthermore, Frontex is monitoring the situation in Ukraine and is in talks with all Member States neighbouring Ukraine. The Agency is ready to support them with officers and equipment. (CR)

Joint Operation Terra 2022

At the beginning of February 2022, Frontex launched a new operation at the EU's external land border. Triggered by the increasing migratory movements along the EU's external land borders, "Operation Terra 2022" is supposed to help EU Member States in the fight against migrant smuggling, trafficking in human beings, drugs smuggling, identifying stolen vehicles, document fraud and terrorism. The operation takes place across 12 EU Member States and covers 62 border crossing points. More than 450 standing corps officers from 28 EU and Schengen countries support national authorities with border management. Operation Terra follows up Frontex land operations that were carried out in the previous years under two separate schemes. The new operation, coordinated from the Frontex headquarters in Warsaw, brought them together under one umbrella. (CR)

First Frontex-led Return Operation

On 25 January 2022, for the first time, Frontex conducted a return operation that was fully initiated and organised by the Agency itself. Upon request and decision of a Member State, Frontex is now able to conduct such operations for the Member State. The operation of January 2022 involved the return of 40 Albanian citizens from Madrid to Tirana. Frontex's service for return operations include:

- Dealing with technical and operational assistance in the organisation and coordination of return operations;
- Providing support in determining the identity of returnees;
- Cooperating with EU Member States and non-EU countries as well as other stakeholders involved in return management;
- Chartering airplanes;
- Engaging return officers from the European Border and Coast Guard standing corps;
- Taking over the contacts with the countries of return.

The decision about who should be returned remains the responsibility of the judicial or administrative authorities of the Member States. (CR)

Agency for Fundamental Rights (FRA)

Tackling Disinformation on the Internet

At the end of February 2022, the FRA published an information video on how to tackle disinformation on the Internet. The practical guide consists of six key messages:

- To convey messages of hope instead of fear;
- To identify why a source is spreading information;
- To use personal storytelling to counter us-versus-them narratives;
- To find new ways to reach the targeted audience;

- To encourage the audience to help share reliable information;
- To stay one step ahead of disinformation campaigns.

The video aims at supporting human rights defenders. (CR)

Specific Areas of Crime / Substantive Criminal Law

Protection of Financial Interests

CJEU Dismisses Actions against Rule-of-Law Conditionality to Safeguard the EU Budget

spot light

On 16 February 2022, the CJEU dismissed the actions brought by Hungary and Poland that sought annulment of Regulation 2020/2092 "on a general regime of conditionality for the protection of the Union budget". The Regulation 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. For a background of the Regulation, the case before the CJEU, and the Advocate General's opinion →eucrim 4/2021, 214–215 and eucrim 1/2021, 19 and eucrim 3/2020, 174–176.

In their actions, Hungary and Poland mainly put forward three arguments that the Regulation should have made invalid in its entirety. The CJEU, sitting as a full court (i.e. all 27 judges), countered these arguments as follows:

➤ *Lack of legal basis?*

Hungary and Poland submitted that the TEU and TFEU do not provide an appropriate legal basis for the contested Regulation, in particular it could not be based on Art. 322(1) TFEU. The latter provision allows the European Parliament and Council to adopt, by means of regulations, "the financial rules which determine in particular the procedure to be adopted for establishing and implementing the budget and for presenting and auditing accounts".

The CJEU first clarified that the wording and context of Art. 322(1) TFEU cover not only the rules which define how expenditure shown in the budget is to be implemented as such but also, in particular, the rules which determine the control and audit obligations on the Member States. Regarding the argument by Hungary and Poland that the real objective of the conditionality mechanism is to penalise EU countries for rule-of-law breaches through the EU budget, the CJEU emphasised second that the Regulation clearly aims at pursuing the legitimate interest in protecting the Union budget. In this context, the CJEU refers to the close link between the effects of rule-of-law infringements with serious risks to the sound financial management of EU finances.

In addition, the CJEU shared the view that Art. 322 TFEU includes the possibility to establish a "horizontal conditionality" linked to the EU values and is not confined to rules for a specific EU programme or action. The judges in Luxembourg emphasised the importance of the common values on which the EU is founded and which define the very identity of the EU as a legal order common to the Member States. As a result, compliance with theses common values (including the rule of law and solidarity) is a condition for the enjoyment of all rights deriving from the EU Treaties, which is why the EU must also be able to defend those values, within the limits of its powers. The sound financial management of the Union budget may seriously be compromised if a Member State commits breaches of the principles of the rule of law.

Considering the genuine link between the establishment of rule-of-law breaches and the protection of the EU's financial interests, the CJEU ultimately rejected the argument that the content of the Regulation is beyond what is necessary for the proper implementation of the Union budget. In conclusion, Regulation 2020/2092 falls within the scope and concept of Art. 322(1) TFEU.

➤ *Circumvention of the procedure laid down in Art. 7 TEU?*

According to Hungary and Poland, only Art. 7 TEU allowed the EU to examine, determine the existence of and impose penalties for breaches of the values enshrined in Art. 2 TEU. Furthermore, the countries claimed that the contested Regulation created a parallel procedure with the same consequences as those stipulated in Art. 7 TEU and thus undermined the institutional balance.

First, the CJEU pointed out that numerous provisions in the Treaties protect the EU values and not only Art. 7 TEU, e.g. Art. 19 TEU as far as the value of the rule of law is concerned. Second, the CJEU ruled that the procedure contained in the Regulation pursues a different aim and has a distinct subject matter than the one in Art. 7 TEU. In addition, the scope of Art. 7 TEU is wider since it not only covers the value of rule of law. Third, the CJEU clarified that, since the Regulation allows the Commission and the Council to examine only situations or conduct attributable to the authorities of a Member State and which appear relevant to the sound financial management of the Union budget, the powers granted to those institutions by that Regulation do not transgress the limits of the powers conferred on the EU.

➤ *Breach of principles of legal certainty?*

In a third plea, Hungary and Poland put forward several allegations that the Regulation is not in line with the EU principle of legal certainty. The countries, *inter alia*, argued that the "rule of law" concept cannot be precisely defined and cannot be given a uniform interpretation, because of "the obligation to protect the national identity of each of

the Member States". Furthermore, a precise assessment is impossible since the Regulation operates with vague terms in the definition of rule-of-law principles in Art. 2(a).

The CJEU opposed this view by stating that, even though the EU respects the national identities of its Member States (as is apparent from Art. 4(2) TEU), the Member States adhere to a concept of "the rule of law" which they share, as a value common to their own constitutional traditions, and which they have undertaken to respect at all times. Accordingly, the principles of the rule of law as listed in Art. 2(a) of the Regulation and developed in the CJEU's case law on the basis of the EU Treaties, are thus recognised and specified in the legal order of the EU and have their source in common values which are also recognised and applied by the Member States in their own legal systems. Consequently, Member States are in a position to determine with sufficient precision the essential content and the requirements flowing from each of the principles stipulated in Art. 2(a) of the Regulation.

Further arguments by Hungary and Poland related to the concept of "serious risk". According to the two countries, the provision that requires that the breaches of the principles of the rule of law which have been found must "seriously risk" affecting the sound financial management of the Union budget or the financial interests of the Union will allow arbitrary penalties to be imposed in uncertain or unproven situations.

The CJEU rejected this argument by pointing to the Regulation that foresees several substantial and procedural requirements to be fulfilled in order to establish the link in question. This includes the condition that a high probability of the occurring risk must be demonstrated and that protective measures must be strictly proportionate to the impact of the breach on the Union budget. In sum, the various provisions of the Regulation meet the requirements of legal certainty.

➤ *Put in focus*

The importance of the judgment is already formally shown that the CJEU delivered the ruling by sitting as full court where the Court considers that a case is of exceptional importance. The CJEU followed the *conclusions by Advocate General Manuel Campos Sánchez-Bordona* delivered on 2 December 2021. The actions for annulment gave the CJEU not only the opportunity to examine the legality of the individual provisions of the Regulation establishing the "conditionality mechanism", but also to provide fundamental statements on the possibilities and powers of the EU to protect its financial interest as well as on the meaning of the common values enshrined in Art. 2 TEU, in particular the value of the rule of law.

Whether the controversial Regulation will now be implemented by the Commission and whether the procedure will finally lead to sanctions against EU Member States where the rule of law is at stake is written in the stars. The Commission has taken the position that it must first establish guidelines for the application of the Regulation. Moreover, it will not be easy to demonstrate the "genuine link" (as emphasised several times by the CJEU) between breaches of the rule of law and the sound financial management of the Union budget. Lastly, one must consider that the Regulation foresees several procedural steps before measures against countries can have real and final effects. (TW)

European Chief Prosecutor: Poland Systematically Refuses Cooperation with EPPO

Following the CJEU's judgment on the validity of Regulation 2020/2092, which ensures protection of the EU's financial interests in cases of rule of law breaches (→page 21), and in view of recital 16 of said Regulation, European Chief Prosecutor *Laura Kövesi* informed the European Commission on 16 February 2022 that Poland refuses to cooperate with the EPPO when it comes to investigations of offences against the EU's financial interests that affect Poland. The country is not participating in the scheme of enhanced cooperation on the establishment of the EPPO, but was also reluctant to apply the regular, binding EU instruments on judicial cooperation, e.g. the European Investigation Order, when the EPPO asked for cooperation to investigate PIF crimes affecting Poland. According to *Kövesi's* letter to the Commission, the EPPO currently has 23 ongoing investigations involving Poland, which is the highest number of any non-participating Member State. Poland also refused to sign a working arrangement with the EPPO, arguing that it must first amend the Polish code of criminal procedure, which would allow recognition of the EPPO as a competent authority. The EPPO is currently unable to collect evidence located in Poland due to this systematic refusal of cooperation. (TW)

Commission Publishes Guidelines on Application of Conditionality Mechanism

spot light

On 2 March 2022, the European Commission published guidelines on the application of Regulation 2020/2092 setting out the general regime of conditionality for the protection of the Union budget (the "Conditionality Regulation"). The Regulation ensures that the EU can financially sanction breaches of the principles of the rule of law that affect or risk affecting the EU budget by EU Member States (→eucrim 3/2020, 174–176). The guidelines come after the CJEU judgments of 16 February 2022 which dismissed actions against the novel EU rules brought by Poland and Hungary (→page 21).

The purpose of the guidelines is to explain more clearly and precisely how the Commission will apply Regulation 2020/2092. They are divided into the following thematic chapters:

- Conditions for the adoption of measures;
- The relation between the Condition-

ality Regulation and other procedures set out in Union legislation to protect the EU budget;
- The proportionality of measures that could be proposed by the Commission;
- Procedure and methodology of the assessment process;
- The protection of the rights of final recipients and beneficiaries.

Regarding the question when the Commission will initiate the procedure set out in the Regulation, the guidelines clarify that the following conditions must be met:
- At least one of the rule-of-law principles referred to in Art. 2(a) of the Conditionality Regulation has been breached in a Member State (these concern, for example, principles of legality, legal certainty, effective judicial protection, separation of powers and equality before the law);
- The said breach concerns at least one of the situations attributable to an authority of a Member State or at least one instance of conduct of such authorities referred to in Art. 4(2) of the Conditionality Regulation, in so far as those situations or that conduct is relevant to the sound financial management of the Union budget or for the protection of the Union's financial interests (authorities could be for example authorities implementing the EU budget and carrying out financial control, monitoring and audit; investigation and public prosecution services; national courts or administrative authorities);
- The said breach affects or risks seriously affecting that sound financial management or those financial interests, covering both revenue and expenditure. There must also be a sufficiently direct relation between the breach and its effect.

The guidelines stress that the Commission will initiate the procedure unless it considers that other procedures set out in Union legislation would allow it to protect the Union budget more effectively. Indicative criteria for more effectiveness of the conditionality mechanism are:
- Scope of the effect and/or extent of risk the breach may entail – for example if other procedures only relate to specific programmes or relate to already materialized effects on the Union budget;
- Types of remedies available and their suitability to different situations to address the relevant breach – for example, if the Union budget is affected in a wide manner due to lack of independence of national courts.

The guidelines define the principles upon which the Commission will carry out its assessments. There will be thorough qualitative assessments on a case-by-case basis, taking due account of the specific circumstances and contexts of each Member State. The assessments will also be carried out in an objective, impartial and fair manner. Assessments will be based on a wide range of evidence and reliable information sources. The latter includes CJEU judgments, reports of the Court of Auditors, the Commission's annual Rule of Law Report and EU Justice Scoreboard, reports of OLAF and the EPPO and information provided by them, as well as conclusions and recommendations of any relevant international organisations and networks (e.g. the CoE bodies GRECO and the Venice Commission). Another important source will be complaints by any third party. For this purpose a complaint form is available on the Commission's website.

The guidelines further explain the different steps of the formal procedure under the Conditionality Regulation, from sending out a written notification to the Member State concerned to the proposal of measures to the Council and their adoption. The procedure for lifting measures is also set out.

A key principle in the application of the Conditionality Regulation is that the final recipients and beneficiaries of EU funding should not be affected by measures taken under the regulation. To ensure that, the Member States concerned by the regulation should continue to make any payments due to these recipients or beneficiaries. If the Member States concerned refuses to honour their obligations, the beneficiaries or final recipients should first turn to the competent national authorities. If this is not possible or does not lead to the expected outcome, they can address the Commission. (TW)

Conditionality Mechanism: MEPs Dissatisfied – Commission Takes Action against Hungary

In a resolution adopted on 10 March 2022, the European Parliament (EP) again criticised the Commission for not having adequately responded to the CJEU rulings on the Conditionality Regulation of 16 February 2022 (→page 21). In this ruling, the Court confirmed the legality of the new EU rules that allow financial sanctioning of Member States in cases of rule-of-law breaches (→eucrim 3/2020, 174–176).

MEPs called on the Commission "to take urgent action" and immediately apply the Rule of Law Conditionality Mechanism by sending a written notification under Art. 6(1) of Regulation 2020/2092 to Member States which continue severe violations of the rule-of-law principles.

The resolution also "regrets the inability of the Council to make meaningful progress in enforcing the Union's values in ongoing Article 7 procedures in response to the threats to common European values in Poland and Hungary". The French Council Presidency is called on to fulfil its commitment to "a humane Europe", i.e. to stand up for strengthening the rule of law and protecting fundamental rights.

The resolution ultimately stressed that any risks of misuse of EU funds or rule-of-law breaches must be excluded before approving national plans under the Recovery and Resilience Facility.

The EP has been at odds with the Commission and the Council for some time over how quickly the novel rules linking rule-of-law breaches with the protection of the EU's budget (con-

cluded at the end of 2020) should be applied. In October 2021, the Parliament launched an action against the Commission over its failure to apply the regulation and for its attempt to "play for time" (→eucrim 4/2021, 215).

The Commission explained that it has been applying the regulation since January 2021 and requested information from Poland and Hungary. On 5 April 2022 – two days after the general elections in Hungary – Commission President *Ursula von der Leyen* told MEPs that the next step in the procedure against Hungary will be taken and a formal letter will be sent to the Hungarian government triggering the conditionality procedure. (TW)

CJEU Rules on Member States' Liability in the Event of Losses of Own Resources

spot light

On 8 March 2022, the CJEU, sitting in for the Grand Chamber, delivered an important ruling on the obligations of EU Member States to protect the EU's financial interests (Art. 325 TFEU) and to apply the EU's customs legislation.

➤ *Facts of the case*

In the case at issue (C-213/19), the Commission brought an action against the United Kingdom for failure of its obligations under EU legislation on control and supervision in relation to the recovery of own resources and under EU legislation on customs duty and VAT. The cases date back to 2007, 2009, and 2015 when OLAF detected risks of extreme undervaluation of imports of textiles and footwear from China by shell companies circumventing the EU customs duties. OLAF and the Commission developed risk assessment tools and anti-fraud strategies and recommended the UK authorities using this EU-wide risk approach. However, according to OLAF, the UK did not follow its recommendations, instead releasing the products concerned for free circulation in the internal market without conducting appropriate customs controls. As a result, a substantial proportion of the customs duties due were not collected or made available to the Commission. Against this background, the Commission initiated an infringement procedure against the UK for not having taken effective control measures on undervalued importation within the period between November 2011 and October 2017. In addition, the Commission requested the correct determination of the customs value.

➤ *Admissibility of the action*

The CJEU first clarified that it has jurisdiction in the case despite Brexit. According to the agreements between the EU and the UK, the CJEU continues to have jurisdiction in any proceedings brought against the United Kingdom before the end of the transition period, i.e. 1 January 2021; the CJEU can also rule on the interpretation and application of EU legislation on own resources relating to the financial years until 2020.

➤ *Breaches regarding the protection of the EU's financial interests*

On the merits, the Court largely upholds the Commission's pleas. As far as the UK's failure to fulfil obligations to protect the EU's financial interests and to counter fraud was concerned, the judges in Luxembourg reiterate the obligations under Art. 325(1) TFEU:

- Member States must not only provide for the application of appropriate penalties, but also of effective and dissuasive customs control measures, in order to effectively and comprehensively collect traditional own resources in the form of customs duties;
- The Member States' latitude and freedom of choice as to the measures to be taken have its limits in the principles of proportionality, equivalence and effectiveness, and general principles;
- Member States have precise obligations as to the result to be achieved;
- The nature of the necessary customs control measures cannot be determined in an abstract and fixed manner, since they depend on the characteristics of EU fraud or other illegal activity, which may change over time.

Considering the particular features of undervaluation fraud, the CJEU concluded that the UK "manifestly failed" to respect the principle of effectiveness under Art. 325(1) TFEU by limiting customs controls to post-clearance action to recover duties. Regarding the breach of obligations under EU customs legislation, the CJEU acknowledged that the risk profiles and types of customs control which OLAF and the Commission were recommending have a non-binding nature. However, the UK was required, at the very least, to take due account of them when establishing its system of risk analysis and risk management during the infringement period. This follows from the duty of cooperation and must apply in particular if Member States have not developed national criteria that are at least as effective as those recommended by the EU. As a consequence, the UK mainly neglected three issues:

- Applying pre-clearance risk profiles to goods before release for free circulation;
- Systematically demanding guarantees in respect of the imports in question;
- Entering in the accounts in due time the amounts corresponding to the difference between the duties calculated on the basis of incorrectly declared values and the duties which would have been established if they had been calculated on the basis of the true value of the goods concerned.

➤ *Breaches regarding obligations to make available own resources*

The CJEU clarified that the UK also infringed EU legislation on own resources since, during the infringement period, the country did not make available to the Commission the traditional own resources in respect of the relevant imports that were due. In this regard, the Court points out that the Member States must establish a Union entitlement to own resources as soon as their authorities are in a position to calculate the amount of duty resulting from a customs debt and to determine the person liable for payment of the duty; they must then

take all necessary measures to ensure that the Union's own resources are made available to the Commission. The management of the Union's own resources system is thus entrusted to the Member States and is their sole responsibility. Because of the direct link between the collection of revenue from customs duties and the making available of the corresponding resources to the Commission, the Member States are obliged to protect the Union's financial interests and to take the necessary measures to ensure the effective and complete collection of customs duties.

In the present case, the CJEU particularly blamed the UK for not determining an accurate value of the imported undervalued goods before their release for free circulation. Thus, the UK created an irreversible situation leading to considerable losses of own resources for the EU, for which the UK must be held liable.

The CJEU then established the liability of the UK for the losses of the EU in the context of OLAF's joint customs cooperation "Snake" and identified several administrative failures by the UK customs authorities to correctly determine the customs value due. Ultimately, however, the Court criticised the Commission's calculation of the amount of losses of own resources.

➤ *Reaction by OLAF*

In a statement of 10 March 2022, OLAF welcomed the CJEU's judgment in the UK undervaluation case. OLAF Director-General *Ville Itälä* said that the judgment validates OLAF's investigative work. He above all expressed pride that the judgment endorsed the methodology which OLAF developed to fight undervaluation and which now could become the main reference tool for all national customs authorities. (TW)

First Annual Report on Implementation of RRF

On 1 March 2022, the Commission published its first annual report on the Recovery and Resilience Facility (RRF). The RRF is providing up to €723.8 billion (in current prices) of grants and loans to Member States to support transformative investments and reforms that boost the EU's economy after the COVID-19 crisis (→eucrim 3/2021, 151).

The report takes stock of the progress made since the establishment of the RRF Regulation in February 2021. It concludes that major advancements have been made and implementation is firmly on its way. The Council adopted 22 recovery and resilience plans, which account for a total of €445 billion. The Commission disbursed €56.6 billion in pre-financing and €10 billion in a first payment in 2021.

The report also includes several examples of the investments and reforms financed by the RRF, which cover the six policy pillars defined in the RRF Regulation, including the European green deal and digital transition. (TW)

ECA Report on EU Support for the Rule of Law in the Western Balkans

On 10 January 2022, the European Court of Auditors (ECA) published a special report "EU support for the rule of law in the Western Balkans: despite efforts, fundamental problems persist". According to the report, the EU has adopted a definition of the rule of law that is enshrined in Art. 2 TEU as one of the common values of its Member States. It is also an essential and necessary condition for EU membership. The ECA audited whether EU support for the rule of law in the Western Balkans (Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia) during the 2014–2020 period has been effective and assessed whether the support was well designed and achieved the planned results.

The Western Balkans receive financial assistance through the Instrument for Pre-accession (currently IPA II). The Western Balkans received about €0.7 billion from 2014 to 2020 in order to support the rule of law and fundamental rights.

The ECA found that, while EU action has contributed to reforms in technical and operational areas (e.g. improving the efficiency of the judiciary), it has had little overall impact on fundamental rule-of-law reforms in the Western Balkans. The ECA points to insufficient domestic political will as the reason for the lack of change and reform.

Following these findings, the ECA made the following recommendations to the Commission and the European External Action Service (EEAS):

- Strengthen the mechanism for promoting rule-of-law reforms in the enlargement process;
- Intensify support for civil society engaged in rule-of-law reforms and media independence;
- Reinforce the use of conditionality in IPA III;
- Strengthen project reporting and monitoring. (AP)

Corruption

EP Pushes for Efforts against Corruption in the World

In a recommendation adopted on 17 February 2022, the European Parliament (EP) addressed several recommendations to the Council and the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy concerning corruption and human rights. MEPs, *inter alia*, advocate a comprehensive EU anti-corruption strategy. This should include a human rights-based approach in the fight against corruption, with victims of corruption placed at its core and the fight against corruption at the centre of the EU's policies promoting democracy, human rights and the rule of law around the world. Work on an internationally agreed definition of corruption should be launched. Furthermore, more efforts are needed to ensure transparency, which includes the abolition of excessive rules on professional secrecy in relevant sectors, the automatic exchange of informa-

tion on tax fraud and evasion, and multinational public registers on beneficial ownerships. Other recommendations include:

- Applying the highest ethical and transparency standards in EU funding;
- Integrating binding and enforceable human rights and anti-corruption clauses into all trade and investment agreements between the EU and third countries;
- Establishing common EU rules for criminal sanctions for corruption on the basis of Art. 83 TFEU;
- Making efforts in freezing and confiscating stolen assets and proceeds of corruption;
- Increasing financial support to civil society organisations that are committed to prevent and fight corruption – including support against strategic lawsuits against public participation (SLAPP suits);
- Establishing binding EU rules on human rights and environmental due diligence, imposed on all entities and business relationships throughout a company's value chain;
- Developing an action plan to strengthen human rights due diligence in sectors such as finance, accounting or real estate, which often foster global corruption.

MEPs also repeated requests to amend the current EU Global Human Rights Sanctions Regime by extending its scope to include acts of corruption or alternatively come forward with a legislative proposal to adopt a new thematic sanction regime against serious acts of corruption. (TW)

Money Laundering

AG Opinion on Public Access to Information on Beneficial Owners

In its opinion of 20 January 2022, Advocate General (AG) *Giovanni Pitruzzella* concluded that the fourth anti-money laundering (AML) Directive (Directive 2015/849) as amended by the fifth AML Directive (Directive 2018/843) is partly invalid. The case concerns in essence the question of finding the right balance between, on the one hand, transparency requirements concerning beneficial owners and the control structures of companies for the prevention and fight against money laundering and terrorist financing, and, on the other hand, the respect for the beneficial owners' fundamental rights, in particular their rights to privacy and protection of their personal data.

➤ *Background of the case*

In the cases at issue (Joined Cases C-37/20 and C-601/20 – *WM and Sovim SA v Luxembourg Business Registers*), two registered beneficial owners of Luxembourgish companies asked for limiting access by any member of the general public to their data because disclosure of that data would entail a disproportionate risk infringement to their fundamental rights. The Luxembourgish authority responsible for the registrations denied the request. The *tribunal d'arrondissement de Luxembourg* referred several questions to the CJEU regarding the validity and interpretation of Art. 30 of the AML Directives. This provision regulates which information on beneficial ownerships must be collected and registered in central registers of the EU Member States. According to Art. 30(5), Member States must ensure that certain data on beneficial owners are accessible in all cases, *inter alia*, to any member of the general public. Member States can grant access to further data. Art. 30(9) provides for an exemption to the access referred in exceptional circumstances to be laid down in national law. This is the case if the access would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation.

➤ *The AG's opinion*

The AG first stressed that the public access to the data constitutes an interference into the beneficial owners' fundamental rights, although this interference is not particularly serious. Second, the AG verifies whether the limitation to the fundamental rights (notably Arts. 7 and 8 of the Charter) can be justified. In this context, he identified two problematic points in the provision of Art. 30 of Directive 2015/849 as amended by Directive 2018/843:

- Regarding Art. 30(5), the EU legislature failed to identify the scope and nature of personal data in clear and precise manner when it left to the EU Member States the possibility to make accessible to the member of the general public additional information on beneficial ownership – in this respect, the AML Directive is invalid;
- Regarding Art. 30(9), it is necessary that the establishment of exemptions cannot be read as being in the discretion of Member States only (as worded in the Directive), but it is an obligation for Member States to implement exemptions in their national law. In this context, the AG acknowledged the purpose to provide access of beneficial ownership data to the members of the general public (without persons/organisations having to demonstrate a legitimate interest anymore), but this must be flanked by appropriate safeguards for the beneficial owners' fundamental rights.

In conclusion, AG *Pitruzzella* considers, however, the access scheme to beneficial ownership information established by the fourth and fifth AML Directives in line with EU fundamental rights law. (TW)

EBA's Second Report on Performance of AML/CFT Banking Supervision

On 22 March 2022, the European Banking Authority (EBA) published the main findings of the second round of reviews of authorities' approaches to the supervision of banks regarding anti-money laundering and countering the financing of terrorism (AML/CFT). These review reports are part of the EBA's new duties to ensure consistent and effective application of the EU's AML/CFT law. For the first report and more background information →eucrim 1/2020, 16.

In the second round, the EBA peer reviewed seven competent supervisory authorities in seven EU/EEA Member States from 2020 to 2021. The review report concluded that the sample triggered similar results as in the first report. All reviewed competent authorities had undertaken significant work to implement a risk-based approach to AML/CFT. AML/CFT supervisory staff in all competent authorities had a good understanding of international and EU AML/CFT standards and were committed to the fight against financial crime. All authorities had started to put in place mechanisms to exchange information with other relevant authorities at home and abroad.

However, the authorities face similar common challenges as those reviewed in the first round, e.g.:

- Difficulties relating to the identification and assessment of ML/TF risks associated with the banking sector and with individual banks;
- Translating ML/TF risk assessments into risk-based supervisory strategies;
- Using available resources effectively, including by ensuring sufficiently intrusive on-site and off-site supervision;
- Taking proportionate and sufficiently dissuasive enforcement measures to correct AML/CFT compliance weaknesses.

It was also found that cooperation with FIUs was not always systematic and continued to be largely ineffective in most Member States. (TW)

Tax Evasion

CJEU: Fines for Failure to Declare Assets Abroad Can Be Disproportionate

On 27 January 2022, the CJEU declared Spanish legislation, which allows the imposition of high fines if a Spanish tax resident failed to comply with mere obligations to declare or purely formal obligations regarding his/her overseas assets, not in line with the principle of free movement of capital (Case C-788/19, *Commission v Spain*).

Under Spanish legislation, Spanish taxpayers who fail to declare or who make a partial or late declaration of assets and rights that they hold abroad are liable for additional assessment of the tax due on the amounts corresponding to the value of those assets or of those rights, including where they have been acquired during a period that is already time-barred. Furthermore, the residents are faced with the imposition of a proportional fine and specific flat-rate fines in such cases.

The judges in Luxembourg acknowledged that the Spanish legislation is appropriate to attain the objectives pursued, i.e. to guarantee the effectiveness of fiscal supervision and to prevent tax evasion and avoidance. In this context, the CJEU pointed out that, despite the existence of mechanisms for the exchange of information or administrative assistance between the Member States, tax authorities principally have less information available on assets held by the tax residents abroad than on those located in the state's territory. However, the CJEU found that the Spanish legislation in question goes beyond what is necessary to achieve said objectives and reprimands mainly three issues:

- The tax authorities' power to make an additional assessment of the tax due without that assessment being subject to any time limit, which undermines the fundamental principle of legal certainty;
- The imposition of a proportional fine of 150% of the tax calculated on amounts corresponding to the value of those assets or those rights held overseas, which can be cumulated with flat-rate fines and which gives the non-compliance with declaratory obligations a highly punitive nature;
- The imposition of flat-rate fines in cases of assets abroad, whose total amount is not capped and is disproportionate to the penalties imposed in respect of similar infringements in a purely national context.

The CJEU concluded that the Spanish legislation is a disproportionate restriction on the free movement of capital. The ruling follows an infringement action brought by the Commission against Spain. (TW)

Counterfeiting & Piracy

Intellectual Property Crime Threat Assessment 2022

On 16 March 2022, Europol and the European Union Intellectual Property Office (EUIPO) published their new Intellectual Property Crime Threat Assessment 2022. The report looks at the threat the EU faces from intellectual property (IP) crime. Key developments identified include the increased production and distribution of counterfeit goods during the COVID-19 pandemic. Detections of counterfeit goods by customs authorities at the EU's borders and on the internal market have decreased, however, from approximately 76 million items detained in 2019 to 66 million in 2020. The report also notes an increasing use of express transport services, particularly via small parcels, which is supposedly related to the growth of online marketplaces. While most counterfeit production takes place outside of the EU, more and more production sites are also being discovered in the EU Member States themselves. The range of counterfeit products varies and includes both luxury items and everyday products, such as the following:

- Clothes, accessories, and luxury goods;
- Electronic/electrical devices, mobile phones and components;
- Food and drink; counterfeit perfumes, and cosmetic products;
- Pesticides;
- Counterfeit pharmaceutical products;
- Digital piracy products;
- Tobacco products;
- Toys.

While IP crime constitutes a substantial threat to the health and safety of consumers, it also negatively impacts the EU economy, with counterfeit and

pirated goods worth €119 billion having been imported into the EU in 2019, representing up to 5.8 % of EU imports in that year.

It is the second joint Europol-EUIPO IP threat assessment report. The first one was published in 2019 (→eucrim 2/2019, 97–98). (CR)

Operation LUDUS II Seizes More than 5 Million Fake Toys

On 24 March 2022, OLAF and Europol reported on the results of the second edition of operation "LUDUS". For the first edition →eucrim 1/2021, 13. The operation targets the trafficking of fake toys and other goods. The operation was led by Spanish law enforcement authorities and Romanian police; it involved 17 EU Member States and 4 third countries (Cote d'Ivoire, North Macedonia, the United Kingdom and the United States). LUDUS II was carried out between October 2021 and January 2022. Law enforcement authorities performed checks and inspections of suspicious shipments and storages; they also carried out online investigations on e-commerce platforms.

As a result, operation LUDUS II led to seizures of over 5 million fake and illegal toys worth nearly €18 million. 99 individuals were reported to judicial authorities, and over 1400 individuals reported to administrative/health authorities; 30 websites were shut down.

OLAF supported checks of customs documentation and performed data analysis. Europol coordinated the operational activities, facilitated the communication exchange and provided operational analysis.

Europol and OLAF stressed that the fake toys did not only infringe intellectual property rights, but also posed a threat to children's' health and safety, e.g. by containing chemicals or risking strangulation, choking, electric shocks, damage to hearing and fire hazards.

The information on the results of operation LUDUS II comes along with an analysis report by Europol on the first edition of operation LUDUS. (TW)

Organised Crime

EU and Latin American Countries Improve Cooperation in Fighting Transnational Organised Crime

On 3 March 2022, the Ministers of the Interior of the Member States of the European Union and Ministers in charge of security matters of the Member States of the Latin American Committee for Internal Security (CLASI) adopted a joint declaration on the fight against transnational organised crime with a particular focus on drug trafficking. The joint declaration starts a new dialogue between the EU and Latin American countries in order to develop a common cooperation culture at the political, technical and operational level.

In the short term, a temporary counter narcotics task force is to be established whose mandate will be to launch joint operations on the basis of shared threat assessments. Furthermore, common operations will identify and seize criminal assets linked to drug trafficking within the framework of the EU's EMPACT cooperation platform.

In the medium term, it is planned to launch a network of law enforcement officers specialised in the fight against drug trafficking between the Latin American States and the EU Member States. This network will also operate together against the use of encrypted networks and other digital tools by organized criminal groups. (TW)

Proposal for a European Union Drugs Agency

On 12 January 2022, the European Commission published a proposal for the creation of a European Union Drugs Agency. The proposed Regulation provides for a targeted revision of the mandate of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).

The EMCDDA, established in 1993 and based in Lisbon, aims at providing the EU and its Member States with factual, objective, reliable, and comparable information (at the European level) on drugs and drug addiction and their consequences. To achieve this objective within its areas of activity, the Centre collects and analyses existing data, disseminates data, improves data-comparison methods, cooperates with European and international bodies/organisations and with third countries, and informs the competent authorities of the Member States of new developments and changing trends.

The proposed Regulation revises the organisation and capabilities of the EMCDDA, giving it a stronger role in combating the challenges posed by drugs in the EU. Under the enhanced mandate, the European Union Drugs Agency would have better monitoring and threat assessment capabilities. A network of forensic and toxicological laboratories would be established to pool the expertise of national laboratories. The role of the national focal points would be reinforced, given that they will provide the new Agency with the respective data. In addition, the Agency would be mandated with developing EU-level prevention and awareness-raising campaigns, with issuing alerts if particularly dangerous substances become available on the European market, and with monitoring and addressing the use of poly-substances (i.e. the addictive use of other substances when linked to drug use).

Ultimately, the international role of the Agency would be strengthened. Following the legislative procedure, the proposal will now be discussed by the Council and the European Parliament. (CR)

Racism and Xenophobia

Council Backs Commission's Initiative to Extend List of EU Crimes to Hate Speech and Hate Crime

On 4 March 2022, the Justice Ministers of the EU Member States discussed the Commission's initiative of December 2021 to include hate speech and hate crime into the list of EU crimes in Art.

83 TFEU (→eucrim 4/2021, 221). According to the Council's press release after the meeting, "a very broad majority was in favour of this initiative". The French Presidency stressed the importance of the subject matter and affirmed that it will continue work on the proposal in order to quickly reach the required unanimous agreement in the Council, as foreseen in Art. 83(1) subpara. 3 TFEU. The European Parliament must consent to the inclusion. (TW)

Council Conclusions on Combating Racism and Antisemitism

On 4 March 2022, the Council of the European Union adopted Conclusions on combating racism and antisemitism. They endorse the EU Strategy on combating antisemitism and fostering Jewish life and invited Member States to develop national action plans and/or strategies in this regard. The conclusions follow the declaration of the French Presidency of the Council of the European Union to make the counteracting of racism and antisemitism one of the political priorities of its current presidency.

The Council censures the alarming increase in racist and antisemitic incidents in the Member States as well as the exacerbation of racist and antisemitic hate crimes and hate speech, Holocaust denial and distortion, and conspiracy myths – both online and offline. It notes that racism and antisemitism may lead to and have led to forms of violent extremism and terrorism.

The Council welcomed the Commission's creation of the Subgroup for the national implementation of the EU Anti-racism Action Plan 2020–2025, which brings together the Member States' representatives and the EU permanent forum for anti-racism civil society organisations. It also welcomed the creation of a permanent structure bringing together the Member States, representatives of the Jewish communities, and relevant interested parties in the form of a working group. The working group will address how to implement the strategy on combating antisemitism and fostering Jewish life and organise an annual civil society forum on antisemitism.

Bearing in mind the principle of subsidiarity, the Council invites Member States to:

- Develop national action plans and/or strategies, as envisaged in the 2020 EU Anti-racism Action Plan and the2021 EU Strategy on combating antisemitism and fostering Jewish life (adopted by the European Commission);
- Endorse and use the non-legally binding working definitions of antisemitism and of Holocaust denial and distortion adopted by the International Holocaust Remembrance Alliance (the IHRA-Definition) as guidance for education and training purposes, including guidance for law enforcement and judicial authorities;
- Raise awareness among the Member States' populations on the fight against all forms of racism and antisemitism by upholding the duty to remember the victims of racist and antisemitic violence and hate crimes, including educating the general public on the historic and contemporary expressions of racism, slavery, and the Holocaust;
- Promote (including financially) education, research, and knowledge of Jewish life, antisemitism, and the Holocaust as well as of racism and slavery;
- Consider developing a common methodology for quantifying and qualifying racial and antisemitic incidents and comparing them both over time and between Member States;
- Ensure that national coordinators or coordination mechanisms for combating racism and antisemitism, public bodies and institutions, equality bodies as well as relevant stakeholders, such as the social partners, civil society organisations/groups involved work closely together in developing preventive measures and evaluating the effectiveness of such measures;
- Strengthen the ability of national investigative and judicial authorities to prosecute illegal online, racist and antisemitic hate crimes and hate speech, in compliance with freedom of expression, including the establishment of measures such as national online monitoring centres and platforms where people can report hateful content.
- Condemn all forms of discrimination based on real or perceived ethnic origin or religious beliefs; ensure an adequate judicial response in compliance with Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law. (AP)

EP Resolution on the Fight against Racism

On 8 March 2022, the European Parliament adopted a resolution on the fight against racism in the media, sports, and schools.

The MEPs proposed stopping EU and state funding for media outlets that competent authorities find to be promoting hate speech and xenophobia – in order to stop the spread of stigmatising narratives that dehumanise members of particular ethnic or racial groups. To increase the penal response to the spread of hate speech, they also proposed that all national audiovisual regulators should be provided with the power to penalise programmes that promote such content.

By insisting on a "zero-tolerance approach" to racism, hate speech, and violence in sports, the MEPs urged the Commission and Member States to adopt effective penalties and to support victims. Athletes who denounce racism or speak out on behalf of diversity need to be protected from retaliation. The Commission must therefore develop guidelines to combat racism in sports at the local, national, and European levels.

With regard to schools, the MEPs called for a revision of education curricula in order to combat bias and eradicate stereotypes that lead to discrimination in today's age. They stressed that racial and ethnic segregation still exists in the education systems of some EU countries and that it needs to be eliminated.

Member States should offer learning programmes to teaching staff, civil servants, and state security forces in order to eliminate racist and xenophobic behaviour at all levels. (AP)

Procedural Criminal Law

Procedural Safeguards

French Presidency Put Access to Lawyer on Agenda

Against the background of continuous attacks on lawyers, the French Council Presidency initiated a debate on protecting access to lawyers and the rule of law. In a discussion paper of 17 February 2022, the Presidency stressed the importance of the independence and professional integrity of lawyers for the rule of law, outlined issues of increasing disrespect to the legal profession and referred to the current (binding and soft law) instruments that are designed to protect the legal profession. On this basis, the French Presidency posed the question of whether a European statute for lawyers, guaranteeing independent practice of the profession, could help to ensure respect for the rule of law. In addition, the Presidency wishes to learn more about the challenges that lawyers face in the EU in their efforts to defend the rule of law, and how the EU could help to address them.

At the JHA Council meeting of 3–4 March 2022, the Justice Ministers had a first discussion on the issues. The French Presidency will further reflect on possible further future steps. (TW)

Data Protection

AG: PNR Directive is in Line with EU Charter

spot light

According to Advocate General (AG) *Giovanni Pitruzzella*, the EU regime for collecting, transferring, processing and retain Passenger Name Records (PNR) for the prevention and prosecution of terrorist offences and serious crime is, in essence, compatible with EU law.

➤ *Background of the case*

The AG's opinion of 27 January 2022 replies to numerous questions that were referred by the Belgian Constitutional Court regarding the validity and interpretation of Directive 2016/681 on the use of PNR data for law enforcement purposes (PNR Directive) and Directive 2004/82 on the obligation of carriers to communicate passenger data (the API Directive) as well as the interpretation of the GDPR in that context. The case is referred to as C-817/19 (*Ligue des droits humains*). Requests for preliminary rulings on the validity of the PNR scheme submitted by German and Slovenian courts are pending (Cases C-215/20 and C-486/20).

In the proceedings before the Belgian Constitutional Court, the Belgium law implementing the PNR and API Directives is challenged. The applicant – the non-profit organisation "*Ligue des droits humains"* – opposed the broad definitions of PNR data and "passengers" which would lead to an indiscriminate and generalised collection of all people travelling to, from and in the EU. Furthermore, the applicant put forward the unclear and imprecise method of pre-screening persons and the long, undifferentiated period of retention of PNR data for five years.

➤ *The AG's opinion*

At first, AG *Pitruzzella* stated that provisions requiring or permitting the communication of personal data of natural persons to a third party (here: public law enforcement authorities) must be classified as an interference with the fundamental rights to private life and protection of personal data. Such interference can only be justified by meeting the requirements of Art. 52 of the Charter. The AG further stressed that it is the onus of the EU legislature to set out the essential elements which define the scope of these interferences. In this context, the AG observes that the EU legislature failed to clearly and precisely define the nature and extent of the data to be transferred by air carriers when it included "general remarks" into the definition of PNR data in point 12 of Annex I of the PNR Directive. Insofar the Directive is invalid.

However, the AG sees no reasons for invalidity as regards first the data that air carriers are required to transfer to Passenger Information Units (PIUs) as such and second the generalised and undifferentiated nature of the transfer of PNR data including the prior assessment of air passengers by means of automated processing. The AG highlights above all the system of safeguards put in place by the PNR Directive. He also takes the view that the CJEU's case law on retention of telecommunication data (*Tele2 Sverige* and *La Quadrature du Net* →eucrim 4/2016, 164 and eucrim 3/2020, 184–186 as well as the article by *Juszczak/Sason*, eucrim 4/2021, 238–266) is not transposable to the PNR case.

Regarding the issues of pre-screening and comparison of PNR data with "other relevant databases", the AG proposed a narrow interpretation of the PNR Directive. Accordingly, the concept of "relevant databases" must be interpreted as covering only national databases managed by the competent authorities and EU and international databases, which:

- have been developed for the purposes of the Directive, i.e. the fighting of terrorism and serious crime, and
- are directly operated by the law enforcement authorities in the course of their duties.

Furthermore, the automated processing of PNR data cannot be carried out by means of machine-learning artificial intelligence systems, which do not make it possible to ascertain the reasons which led the algorithm to establish a positive match.

Regarding the complaint about the data retention period, the AG ultimately proposed that the PNR Directive should be interpreted in accordance with the

Charter. This means that the retention of PNR data provided by air carriers to the PIU for a period of five years is permitted, after the prior assessment has been carried out, only to the extent that a connection is established, on the basis of objective criteria, between those data and the fight against terrorism or serious crime. (TW)

CJEU Rules on Scope of GDPR for Tax Authority Requests

The provisions of the General Data Protection Regulation (GDPR) do not in principle prevent the tax administration from requiring a service provider on the internet to provide it with information on taxpayers, the CJEU ruled on 24 February 2022 in Case C-175/20. However, such data must comply with the data protection principles laid down in Art. 5(1) GDPR, in particular the data requests and transfers must be necessary in view of the specific purposes for which they are collected and the period of time to which the collection of such data relates does not exceed the duration strictly necessary to achieve the objective. Beyond the specific context at issue (requests by the Latvian tax authority to an online advertisement service regarding second hand sales of cars), the ruling is of general relevance for the scope of data protection vis-à-vis requests by public authorities. (TW)

Statewatch Report: Increasing Use of Biometric Technologies at EU Level Drives Forward Ethnic Profiling

The ongoing rollout of biometric identification systems is likely to see ethnic minority citizens and non-citizens subjected to a growing number of unwarranted intrusions into their everyday activities, says a report by Statewatch that was presented at the end of February 2022. "Building the biometric state" examined the development and deployment of biometric identification technologies by police and border forces in Europe over the last two decades. It also includes case studies from France, Italy and Spain demonstrating the challenges to fundamental rights if the technology is more widely used in the EU. According to the report, the increasing use of the technology, which is driven forward by the EU's interoperability plans (→eucrim 2/2019, 103–104), is likely to exacerbate existing problems with racist policing and ethnic profiling.

The report first outlines the gradual development of an overarching biometric identity system at EU level, starting from the establishment of Eurodac (storing asylum-seekers' fingerprints) at the turn of the century, to the ongoing construction of the Common Identity Repository (CIR) within the EU's interoperability framework. Subsequently, it is examined how public funding from the EU's research and innovation programmes has contributed to the development of biometric identification technologies, in particular those that have later been incorporated into initiatives such as "smart borders". In this context, the report states that the EU has awarded some €290 million in public funding to the development of biometric technology since 1998. The majority of research funding has focused on public security applications for biometrics.

The followings sections of the report analyse how the networks of policing refined the use of the new technologies and how they are being deployed using ethnic profiling and easing identity checks.

The authors argue that renewed efforts on multiple fronts are needed to ensure that state authorities are held publicly and politically accountable and it is necessary to develop alternatives to the status quo. Potential measures should include:

- "Know your rights" campaigns and community organising;
- Administrative and legal complaints to uphold privacy and data protection rights;
- Adequate resources and independence for data protection authorities;
- "Firewalls" between policing and public services;
- Critical research and investigative journalism to inform campaigns and complaints;
- Publicly-funded research that acts in the public interest;
- Efforts to ensure transparency in law, policy-making and enforcement. (TW)

Commission and US Government Reach Agreement on Principles of Future Trans-Atlantic Data Privacy Framework

On 25 March 2022, the European Commission announced that a preliminary political agreement had been reached on the principles of the future framework for transatlantic data flows. New negotiations with the U.S. government had become necessary after the CJEU toppled the predecessor agreement, the EU-US Privacy Shield, in the 2020 *Schrems II* decision (→eucrim 2/2020, 98–99). The ruling led to great uncertainty in the economic sector, for which the Privacy Shield applied.

The EU and U.S. side could agree on the following key principles:

- A new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security;
- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards;
- A new two-tier redress system to investigate and resolve complaints of Europeans on access of data by U.S. intelligence authorities; this will include a Data Protection Review Court;
- Strong obligations for companies processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the new transatlantic data privacy framework through the U.S. Department of Commerce;
- Specific monitoring and review mechanisms.

Next steps: Agreement was only reached in principle. It must now be translated into a concrete legislative

document that has to be adopted by both sides. U.S. commitments will be included in an "Executive Order". This will form the basis for the European Commission to draft an adequacy decision pursuant to Art. 45 GDPR. Such adequacy decision would facilitate data transfers between EU and U.S. companies. Currently, data transfers can be based on standards contractual clauses which necessitate, however, a complex "transfer impact assessment". (TW)

Victim Protection

Eurojust Report Maps Challenges for Victims' Rights

On 22 February 2022, Eurojust published a report on its casework on victims' rights. The report looks at the main challenges related to the exercise of victims' rights in a cross-border context and at best practices in overcoming them. Issues dealt with in the report relate mainly to the following:

- Definition and identification of victims, especially in cases involving high numbers of victims and/or large-scale terrorist attacks;
- Uncertainties about the procedural status of victims;
- The need to anticipate and mitigate the risk of secondary or repeat victimisation;
- Considerations given to victims' interests when addressing jurisdiction issues;
- Difficulties in ensuring the compensation of victims.

The report makes several recommendations, e.g. to involve Europol at an early stage and to make use of coordination meetings at Eurojust. Information on money flows also often leads to the identification of the names and locations of victims.

Looking at the procedural and protection rights of victims, in particular, the report recommends already discussing victims' procedural rights during the investigation phase – as part of the prosecutorial strategy. It also recommends discussing the setting-up of Joint Investigation Teams, coordination meetings, and coordination centres. To secure effective access to justice, the report outlines several best practices, e.g. to take the victims' interests into consideration when discussing matters of jurisdiction and a possible transfer of proceedings. Many judicial authorities proactively reach out to victims to inform them of their rights and any relevant procedures. In some Member States, victims are provided with free legal aid, representation, and interpretation/translation. In addition, victims are given the possibility to give evidence, to submit requests for action during the investigation, and to be present at the hearings.

Lastly, the report pinpoints Directive 2012/29/EU on Victims' Rights as a key element for "enshrining the victim's dimension in cross-border investigations and prosecutions."

The report is also supporting the European Commission Coordinator for Victims' Rights in mapping the difficulties for victims' rights in the European Union. (CR)

Cooperation

Police Cooperation

Council Declaration on Interpol's Red Notices

At their meeting on 3 March 2022, the Home Affairs Ministers of the EU Member States approved a short declaration on Interpol's red notices. Red notices are the means by which Interpol electronically disseminates requests by national law enforcement authorities to locate and provisionally arrest persons who are wanted for extradition, surrender or similar legal action. Although red notices must comply with Interpol's constitution and rules, some countries abuse them against "politically undesirable persons".

The Council declaration (not yet public) welcomed the progress made by Interpol in setting up internal mechanisms to assess any violation of Interpol's constitution prior to the publication and diffusion of red notices. Interpol is, however, invited to maintain a regular dialogue with the Council working groups and exchange information how the abuse of red notices for political reasons or violation of human rights can be prevented. (TW)

Study on Politically Motivated Interpol Red Notices

On 7 February 2022, the LIBE Committee discussed a study which analysed the EU's possibilities to protect EU citizens from politically motivated Interpol Red Notices.

Red Notices refer to worldwide requests between Interpol states to temporarily detain a person for a serious crime pending extradition. Interpol is not allowed to circulate Red Notices if the requesting states commit human rights violations. For this purpose, internal controls are to be carried out by Interpol. The number of Red Notices has significantly increased in recent years.

The study points out that the risk of politically motivated Red Notices is real and has increased. Despite reforms of the Interpol Red Notice System since 2013, a number of legal tools continue to be lacking and there is a substandard transparency in the processing of Red Notices. Considering the amount of notices in circulation and the current set up, proper legal safeguards cannot be expected to be sufficiently enforced in the near feature.

Against this background, the study makes several recommendations to the EU institutions to improve the handling of Red Notices within the bloc. This includes the request to the Commission to push through concerns by the EU in negotiations with Interpol, such as:

- Production of a forecast analysis and modelling that account for high volume cases and decentralised review;

- Availability of procedural and substantive tools that ensure consistent and transparent processing of requests, reviews, challenges, corrections and deletions;
- Production of annual statistical data on the processing of Red Notice requests;
- Development of public risk profiles of countries requesting Red Notices.

Internally, the EU should improve and better use synergies of platforms that facilitate the information exchange. According to the study, the European Search Portal is already a good starting point but its legal and institutional framework must further be developed. This could include a database on decisions related to Red Notices as well as a repository with relevant and updated human rights information on requesting countries. (TW)

European Arrest Warrant

CJEU: No Carte Blanche to Refuse EAWs from Poland

spot light

In its judgments of 22 February 2022 in the Joined Cases C-562/21 PPU and C-563/21 PPU, the CJEU upheld its case-law on the refusal of European Arrest Warrants (EAWs) issued by Polish authorities if the requested person put forward infringements of fair trial. The case law developed for the possible refusal of EAWs in case of complaints about the independence and impartiality of the judiciary (inherent in the fundamental right to a fair trial) also applies if the right to a tribunal previously established by law is at issue. The judges in Luxembourg stressed that the executing judicial authority must stick to the two-step examination regarding breaches of the requested person's fundamental right to a fair trial but they specified the criteria for this examination.

➤ *The preliminary ruling question*

The CJEU, sitting in for the Grand Chamber, replied to references for preliminary rulings by the *Rechtbank Amsterdam*. In essence, the Dutch court asked under which circumstances a refusal of Polish EAWs is permitted if the panel of judges who adjudicate a criminal case was appointed by the Polish National Council of Judiciary ("the KRS"). The Rechtbank Amsterdam argued that the KRS can no longer be considered an independent body after the judicial reforms that entered into force in 2018. In addition, there is no effective legal remedy for the defendant in Poland (as the issuing Member State) to challenge the validity of the judicial appointment. For more background information on the case and the opinion of the Advocate General →eucrim 4/2021, 227–228.

➤ *Findings of the CJEU upholding the two-step examination*

The judges in Luxembourg reiterated their standing case law on the importance of the principles of mutual trust and mutual recognition for the execution of EAWs. They stressed that a refusal of the execution of an EAW for reasons of fundamental rights infringements is only possible in exceptional circumstances. Moreover, the operationality of the EAW scheme must be ensured, which is why a dialogue between the executing and issuing authority as a consequence of the duty of sincere cooperation must be kept up. Against this background, an executing authority cannot dispense with a specific and precise verification which takes account of, *inter alia*, the requested person's personal situation, the nature of the offence and the factual context, if there is evidence of systemic or generalised deficiencies concerning the independence of the judiciary in the issuing Member State. Even an increase in systemic or generalised deficiencies cannot in itself justify a refusal of the EAW. As developed in previous case law in relation to the rights to an independent and impartial court (→eucrim 2/2018, 104–105 and eucrim 4/2020, 290–291), the executing authority must therefore determine:

- in a first step, a real risk of breach of the fundamental right to a fair trial in the issuing Member State on account of systemic or generalised deficiencies, plus
- in a second step, the concrete impact of the deficiencies on the person's situation, i.e. there must be substantial reasons for believing that that person will run such a risk if he/she is surrendered.

The CJEU justified the necessity to carry out the two-step examination mainly by the following arguments:

- Inextricable links between the guarantees of judicial independence and impartiality and of access to a tribunal previously established by law as parts of the fundamental right to a fair trial (enshrined in Art. 47(2) CFR);
- Need not to undermine the objectives of Framework Decision 2002/584 on the EAW and the principle of mutual trust, notably considering that impunity must be avoided;
- Coherence with the other rule-of-law mechanisms in place, in particular the competences of the European Council and Council in the Article 7 procedure must be respected.

➤ *Clarification of the criteria for examination*

Subsequently, the CJEU specified the detailed rules for applying the two-step examination regarding the fundamental rights at stake in the present case.

Regarding the first step, the executing authority must consider the standard of protection of the fundamental right guaranteed in Art. 47(2) CFR. In this regard, the right to be judged by a tribunal "established by law" encompasses, by its very nature, the judicial appointment procedure. It is stressed, however, that the executing judicial authority must carry out an overall assessment of a number of factors, on the basis of any evidence that is objective, reliable, specific and properly updated concerning the operation of the issuing Member State's judicial system. The fact that a body, such as the KRS, which is involved in the appointment of judges, is made up, for the most part, of members

representing or chosen by the legislature and the executive, is *per se* not sufficient to justify a refusal decision by the judicial authority executing an EAW.

Regarding the second step, the judges in Luxembourg found that, in general, the requested person must adduce specific evidence to suggest that systemic or generalised deficiencies in the judicial system had a tangible influence on the handling of his or her criminal case or are liable, in the event of surrender, to have such an influence. Such evidence can be supplemented, as appropriate, by information provided by the issuing judicial authority. As regards the specific information which must be provided a distinction must be made according to the purpose of the EAW:

- If the EAW was issued for the purpose of executing a custodial sentence information must be provided on the composition of the panel of judges who heard the criminal case, the appointment procedure of the judges concerned and their possible secondment, and the exercise of the right to reject judges as well as the outcome of this request.
- If the EAW was issued for the purpose of conducting a criminal prosecution, the executing authority must rely on information concerning the requested person's personal situation, the nature of the offence for which that person is prosecuted, the factual context surrounding that EAW or any other circumstance relevant to the assessment of the independence and impartiality of the panel of judges likely to be called upon to hear the proceedings after surrender. On this basis, an overall assessment is required whether the person runs a real risk of breach of the fundamental right.

By contrast, the fact that the identity of the judges who will be called upon eventually to hear the case of the person concerned is not known at the time of the decision on surrender or, when their identity is known, that those judges were appointed on application of a body such as the KRS is not sufficient to refuse that surrender.

➤ *Put in focus*

The decided case follows the line of arguments established by the CJEU in the famous "LM" judgment (→eucrim 2/2018, 104–105) and it is closely related to the Joined Cases C-354/20 PPU and C-412/20 PPU which were brought forward by the Rechtbank Amsterdam as well (→eucrim 4/2020, 290–291). The Dutch court fail for the second time with the attempt to reach a wider interpretation of the refusal ground on fundamental rights infringements in an EU Member State which puts maintenance of rule-of-law principles at stake. The judges in Luxembourg deny to give green light to a more or less general halt of judicial cooperation with such countries as they have already done in previous judgments. The main arguments remain the need to avoid impunity and not to interfere into the Article 7 procedure. However, the judgment does not much take into account that impunity could be avoided by transfer of the criminal proceedings. Furthermore, it should be recognised that the Article 7 procedure is currently in a political cul-de-sac since the Council has not taken any decision to determine that there is a clear risk of a serious breach by Poland of the values referred to in Art. 2 TEU.

Another critical point from the defence perspective is the imposition of several duties for the person concerned to produce evidence. This relates to both the first and second step of the examination of whether there is a real risk of a breach of the fundamental rights to a fair trial and of whether this risk will materialise in the concrete situation of the defendant. In sum, in practice, it will hardly be possible to produce the needed, in order to convince the executing judicial authority that the EAW should be refused due to fundamental rights infringements in the issuing country. Thus, the CJEU's case law as established in "LM" will remain a paper tiger. The "success rate" for the defendant will nearly be zero. (TW)

Law Enforcement Cooperation

Progress on E-Evidence Package – Stakeholders Remain Critical

Reaching an agreement on the controversial new EU rules for law enforcement authorities to get quick access to data stored at service providers (legislative proposals on "e-evidence") is one of the priorities of the French Council Presidency. It relaunched the trilogue negotiations on the Commission proposals of 2018 (→eucrim 1/2018, 35–36). In February 2022, the French Council Presidency published the latest trilogue document marking the parts that were provisionally agreed on and the parts on which discussions are ongoing.

On 4 March 2022, the Justice and Home Affairs Ministers took stock of progress in the ongoing negotiations. It was stated that the discussions with the European Parliament (EP) during successive Council presidencies have enabled progress on defining the main structures for a possible compromise text. However, given the substantial divergence between the legislators' positions (→eucrim 4/2020, 295–296 and eucrim 4/2018, 206), it has not yet been possible to reach an agreement on the main components of the envisaged e-evidence package. The main controversial issue remains the question of the procedure for the notification of the e-evidence request by the requesting authority to the authority of the member state of the place of establishment of the private supplier.

In a statement of 4 March 2022, civil society organisations and bar associations stood up for the EP's positions. They particularly support the EP negotiators in the following:

- Treating content and traffic data with the same high procedural protections;
- Denying a residence criterion (i.e. notification only when there are reasonable grounds to believe the person is not residing in the issuing State);
- Including a substantive list of grounds for refusal similar to Art. 11 of the Di-

rective on the European Investigation Order;
- Ensuring consistency with the GDPR;
- Mandatorily notifying the executing state of requests for subscriber data and other identifiers;
- Introducing reasonable deadlines for the emergency procedure;
- Providing for a common European exchange system.

Meanwhile, the French Council Presidency reiterated that the co-legislators agreed to continue their efforts to draft a compromise text. (TW)

New EMPACT Cycle Started – Impact by War in Ukraine

January 2022 saw the start of the new EMPACT cycle 2022–2025 to fight organised and serious international crime. The European Multidisciplinary Platform Against Criminal Threats (EMPACT) is a permanent instrument running in four-year cycles to identify, prioritise, and address threats posed by organised and serious international crime. The platform is driven by the EU Member States and supported by all EU institutions, bodies, and agencies involved in the area of justice and home affairs in a broader sense (e.g. Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA, and EFCA). Third countries, international organisations, and other public and private partners are also associated with the platform.

Priorities for the new EMPACT cycle for the 2022–2025 period include:
- Fight against high-risk criminal networks;
- Cyberattacks;
- Trafficking in human beings;
- Child sexual exploitation;
- Migrant smuggling;
- Drug trafficking;
- Fraud, economic and financial crimes;
- Organised property crime
- Environmental crime;
- Firearms trafficking.

Document fraud is also being addressed as a common, horizontal, strategic goal, given that it is a key enabler for many crimes.

On 22 March 2022, the French Council Presidency informed the Member States and EU bodies that the war in Ukraine will also influence the EMPACT policy. The Presidency put forward a proposal "to activate the 'EMPACT community' in order to assess, anticipate, prevent and counter existing or emerging serious and organised crime threats linked to or entailed by the war in Ukraine, with the support of JHA agencies, EU bodies and institutions". This should be done along the following work strands:
- Intelligence assessment and monitoring: National authorities responsible for leading different EMPACT actions (so-called "drivers") should work actively with Europol and relevant JHA agencies. The received information should be systematically cross-checked and analysed both at the national and EU level with the support of JHA agencies, notably Europol and Frontex. Europol and Frontex should prepare "analytical products";
- Operational response: Drivers should regularly assess operational action plans and think of adjustments if crime threats emerge from the war. After preliminary assessments, the evolution of crime in Ukraine should be taken into account in the EMPACT crime areas.;
- External dimension: Close cooperation of all relevant actors at the external borders (especially customs and border guards) is key for an efficient fight against cross-border crime. Frontex plays a crucial role in this regard as well. The agency is invited to inform the drivers about the situation, the measures taken and the possible support.

The note by the French Presidency expects that the war in Ukraine will have consequences on the crime scene in the EU and that all prority areas of EMPACT will be affected in the short term (e.g. cyberattacks and trafficking in human beings), mid-term (e.g. firearms trafficking and money laundering), and long term (e.g. evolution of criminal organisations). (CR/TW)

Report on JHA Network Activities 2021

At the end of January 2022, Frontex published the final report on the Justice and Home Affairs (JHA) Agencies' Network Activities 2021. Frontex presided the Network in 2021. The activity report summarizes the networks meetings, thematic reports and cooperation of the year 2021. Furthermore, the report outlines the priorities for 2022.

Achievements of the year 2021 include the network's efforts to turn green under the priorities of the European Green Deal. In this context, the Network dealt, *inter alia*, with the links between climate change and organised crime/terrorism and the legal framework and operational aspects of the fight against environmental crime. Another priority in 2021 was to take further steps towards the digitalisation of the JHA Agencies. Thematic issues here included:
- The increasing use of IT systems by the JHA Agencies;
- The development and implementation of new functionalities of EU large-scale IT systems;
- The development of AI and its use in the management of EU external borders and in law enforcement practice;
- The development of information management strategies and possible synergies in this regard between the JHA Agencies.

Another important issue in 2021 was the network's assessment following its 10th anniversary in 2020. The heads of the JHA Agencies endorsed an assessment report that looks at the value of the network in enhancing inter-agency cooperation, implementing the EU priorities in the areas of freedom, security and justice and aligning activities in areas of common interest. While the assessment finds the network to be a very good platform for working-level coordination, it also sets out several recommendations, e.g.:
- Establishing a trio presidency format, in order to discuss overarching topics in a more thorough way and facilitate long-term planning;

- Ensuring adequate budgeting and human resources;
- Adopting new guidelines for the establishment and functioning of working groups and thematic expert meetings;
- Strengthening cooperation with key stakeholders, such as the European Parliament and the Council.

Ultimately, looking at the year 2022, the activity report underlines the need to further implement the recommendations of the 10-years assessment report and to give continuity of established practice. In 2022, the Justice and Home Affairs Agencies' Network is presided by CEPOL. Digitalisation and the green deal will remain priorities in 2022, but CEPOL will elaborate on specific issues in this regard. In addition, cooperation between JHA Agencies and third countries will be the third thematic priority.

The Justice and Home Affairs Agencies' Network (JHAAN) was initiated in 2010 by the Standing Committee on Internal Security (COSI) within the Council. The main objectives are to increase cooperation between the EU bodies involved in justice and home affairs and to explore synergies in areas of common interest. Since 2012, the network comprises nine EU agencies (CEPOL, EASO, EIGE, EMCDDA, eu-LISA, Eurojust, Europol, FRA and Frontex). (CR)

Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases

After several Higher Regional Courts in Germany took the viewpoint that evidence gained from chat messages exchanged between criminals via EncroChat can be used in criminal proceedings in Germany (→eucrim 1/2021, 22–23), the Federal Court of Justice (*Bundesgerichtshof*) handed down the first supreme court judgment in these cases (decision 5 StR 457/21). On 2 March 2021, the Court rejected an appeal on points of law against a conviction by the Regional Court of Hamburg. The Regional Court sentenced the accused to a term of imprisonment of five years for ten crimes of trafficking in narcotics in a not insignificant amount and ordered the confiscation of proceeds of more than €70,000. In some cases, central evidence were text messages sent by the accused via the provider EncroChat to organise drug trafficking. In his appeal, the accused complained, among other things, that this data, obtained from French authorities in 2020 and transmitted to the German authorities, should not have been used as evidence.

➤ *Facts of the case*

In 2017 and 2018, there were indications in France that suspects were carrying out organised drug trafficking via specially encrypted mobile phones ("crypto phones") of the provider EncroChat. With these devices, one could neither make phone calls nor use the internet, but only send chat messages (SMS), create notes or store and send voice messages. Communication was only possible between EncroChat users. Due to a special equipment of the phones and a special encryption technology, law enforcement authorities could neither access the communication conducted with them nor read out the contents of the devices or locate them. The devices were advertised with these features and a guarantee of anonymity. However, they could not be purchased from official sales points, but only from special sellers through anonymous channels at a high price of over €1,600 for a period of use of six months. A legally existing company "EncroChat" could not be found, nor could those responsible for this company or a company headquarters.

The French law enforcement authorities initiated an investigation on suspicion of criminal association, among other things, and found that the encrypted communication between EncroChat users ran via a server operated in Roubaix, France. With authorisation from a French court, they accessed the data on the server. This revealed that over 66,000 SIM cards from a Dutch provider were registered in the system, which were used in a large number of European countries. A decryption of several thousand "notes" from EncroChat users proved that they were undoubtedly linked to illegal activities, such as drug trafficking in particular, with up to 60 kg of cocaine.

At the request of the French public prosecutor's office, a court in France authorised the installation of an interception device on the data passing through the French server and stored on the phones as of 1 April 2020. According to initial findings, 63.7% of the phones active in France were certainly used for criminal purposes, the remaining devices (36.3%) were either partly inactive or not yet evaluated. After evaluating the data obtained in the first month, the public prosecutor's office and the court assumed that the EncroChat users were "almost exclusively criminal clientele".

The operation was assisted by Europol and Eurojust. Europol forwarded data to the Federal Criminal Police Office (*Bundeskriminalamt*) since it was found that a large number of serious crimes had been committed by EncroChat users in Germany. The Central Office for Combating Internet Crime at the General Public Prosecutor's Office in Frankfurt am Main then initiated investigations against "unknown persons". In these pre-trial proceedings, a European Investigation Order addressed to France was issued on 2 June 2020 with the request to transfer the EncroChat data concerning Germany and to allow its use in German criminal proceedings. Both were approved by a French court on 13 June 2020.

➤ *Decision by the Federal Court of Justice*

The EncroChat cases encountered fierce criticism in German legal literature arguing that interception of telecommunications against a mass of people without concrete criminal suspicion would not have been possible under German law and law enforcement authorities disregarded the rules of mutual legal assis-

tance in criminal matters, as a result of which the utilisation of evidence should be prohibited. The FCJ, however, dismissed these arguments.

First, the Court reiterated its case law on the use of evidence collected abroad:
- The question of whether such a prohibition exists is exclusively governed by German law;
- A review of the investigative measures (here: the French one) against the standard of foreign law does not take place.

This means that it is therefore not decisive whether a measure carried out in France, as in this case, solely according to French law could also have been ordered in Germany. Furthermore, review of foreign law is not a prerequisite for the transfer of evidence obtained by French authorities under French law to German criminal proceedings. The different prerequisites for ordering in France and Germany can be compensated for at the level of utilisation of evidence in accordance with section 261 of the German Code of Criminal Procedure.

Second, the FCJ found no violation of fundamental values of human rights or European law or of fundamental requirements of the rule of law in the sense of the "ordre public" to be examined in mutual legal assistance, which could lead to a prohibition of the utilisation of evidence. The FCJ stressed above all that, according to the information available to the French authorities after the first access to the data, the investigations did not involve the mass surveillance of a large number of mobile phone users, even without suspicion. Rather, EncroChat presented itself to the French authorities as a network that was designed from the outset to support criminal activities and operated in secret. Based on the initial findings of an almost exclusively criminal use of such phones, a user was therefore already suspicious of criminal activities in the field of organised crime such as drug and arms trafficking or money laundering simply because of the acquisition of an EncroChat mobile phone, which was not available through normal distribution channels and entailed considerable costs.

Third, the FCJ denied that a possible violation by French authorities of the duty to inform Germany in a timely manner about interception measures affecting the territory of the Federal Republic of Germany (Art. 31 of the EIO Directive) can result in a prohibition of the use of evidence. This already results from the subsequent all-round authorisation of the use of the data. Regardless of this, it is questionable whether the duty to notify serves to protect the individual concerned from the use of evidence in Germany. In any case, the necessary weighing of the different interests would lead to a predominance of the state's interest in criminal prosecution. It is also legally unobjectionable that the Public Prosecutor's Office in Frankfurt am Main applied for a comprehensive transfer of evidence in proceedings conducted against unknown persons on the basis of a general suspicion, which ultimately, however, specifically concerned each user.

Lastly, the FCJ sees no hindrances to accept the evidence in view of the exchange of the information prior to the European Investigation Order. In this context, it is pointed out that cross-border transmission of intelligence for criminal prosecution is readily permissible under the European mutual assistance provisions even without a request for mutual assistance. According to the FCJ, a targeted or systematic circumvention of regulations serving the individual legal protection of accused persons by French or German authorities has neither comprehensibly been demonstrated nor been otherwise concretely evident. (TW)

Council of Europe

Reported by Dr. András Csúri (AC)

Foundations

Human Rights Issues

Russian Federation Ceases to be a Member of the CoE

The Committee of Ministers, acting under Art. 8 of the Statute of the CoE, decided that the Russian Federation would cease to be a member of the CoE after 26 years of membership (as of 16 March 2022). Article 8 of the Statute of the CoE deals with the consequences for membership in the event of violation of Art. 3 ECHR. The events leading up to the decision:
- 28 February 1996: Russia joins the CoE;
- 24 February 2022: Russian military action starts in various parts of Ukraine;
- 25 February 2022: The Committee of Ministers launches the procedure for suspension of a member's rights of representation under Art. 8 of the Statute of the CoE and agrees to suspend the Russian Federation from its rights of representation in the CoE, in accordance with the Committee's relevant Resolution on

legal and financial consequences of the suspension;

■ 1 March 2022: The ECtHR grants an interim measure concerning Russian military operations. The Court considers the ongoing military action to constitute a real and continuing risk of serious violation of the rights of the civilian population as guaranteed by the Convention, in particular under Arts. 2 (right to life), 3 (prohibition of torture and inhuman or degrading treatment or punishment), and 8 (right to respect for private and family life) of the ECHR. Under Rule 39 of the Rules of Court, the ECtHR indicates to the Russian government to refrain from military attacks against civilians and civilian objects, including residential premises, emergency vehicles, and other specially protected civilian objects and to immediately ensure the safety of the medical establishments, personnel, and emergency vehicles within the territory under attack or siege by Russian troops.

■ 10 March 2022: The Committee of Ministers decides to consult the Parliamentary Assembly on potential further use of Art. 8 of the Statute.

■ 15 March 2022: The Parliamentary Assembly unanimously adopts an Opinion, which states that the Russian Federation can no longer be a member state of the Organisation. The government of the Russian Federation informs the Secretary General of its withdrawal from the CoE in accordance with the Statute of the CoE and of its intention to denounce the ECHR.

■ 16 March 2022: The Russian Federation ceases to be a member of the CoE.

■ 16 September 2022: In line with the Committee of Ministers Resolution from 23 March 2022 the Russian Federation will cease to be a High Contracting Party to the ECHR. The ECtHR will deal with applications directed against Russia in relation to alleged violations of the Convention that occurred until 16 September 2022. Russia is bound to fulfil its full financial obligations up to 16 March 2022; it also remains liable for all arrears accrued at that date.

ECtHR Rules on Systemic Dysfunctions in Polish Judiciary

The ECtHR examined anew systemic dysfunctions in the Polish judiciary system in two judgments handed down in February and March 2022.

➤ *Interim measures in the case of Polish Supreme Court judge's immunity*

On 8 February 2022, the ECtHR ordered an interim measure in the case *Wróbel v Poland* (Application no. 6904/22). The applicant, *Włodzimierz Wróbel*, is a well-known critic of the Polish government's judicial reforms. He has been a Criminal Chamber judge on the Polish Supreme Court since 2011. In 2020, he co-authored a resolution of the Supreme Court which held, among other things, that the Disciplinary Chamber of the Supreme Court was not an "independent tribunal established by law", given the involvement of the new National Council of the Judiciary (NCJ) in the appointment procedure of judges to that Chamber.

On 16 March 2021, the State Prosecutor's Office sought the waiver of Mr Wróbel's immunity, with a view to prosecuting him on charges of criminal negligence in connection with a judicial decision rendered in a criminal case. Said decision was given by a three-judge panel of the Criminal Chamber of the Supreme Court. According to the prosecutor, the applicant had failed to fulfill his obligation to verify whether the accused had already served his prison sentence, which resulted in him being unlawfully detained. The request for waiver of immunity was rejected by the Disciplinary Chamber of the Supreme Court on 31 May 2021, which was then challenged by the Public Prosecutor's Office, and a hearing was scheduled for 9 February 2022.

On 4 February 2022, Mr Wróbel applied to the ECtHR under Rule 39 of its Rules of Court to suspend the proceedings pending against him before the Disciplinary Chamber of the Polish Supreme Court. The suspension was to be upheld until the government either fully implements the CJEU's order of 14 July 2021 (Case C-204/21R) and the judgment of that court of 15 July 2021 (Case C-791/19) or appoints a panel of Supreme Court judges recommended by the NCJ operating before 6 March 2018 to hear his case. The applicant further argued that a ruling against him could lead to his suspension, damage his reputation, result in the imposition of restrictive preventive measures, and have a deterrent effect on other judges. He referred to the ongoing crisis of the rule of law in Poland and to Arts. 6 (right to a fair trial) and 8 (right to respect for private and family life) ECHR.

The Court asked that the Polish government ensure that the proceedings concerning the lifting of Mr Wróbel's judicial immunity comply with the requirements of a "fair trial" as guaranteed by Art. 6 (1) ECHR. This particularly concerns the requirement of an "independent and impartial tribunal established by law", and that no decision in respect of his immunity be taken by the Disciplinary Chamber of the Supreme Court until the ECtHR has finally ruled on his complaints. The interim measure also makes reference to the application in *Reczkowicz v. Poland*, (Application no. 43447/19), in which the ECHR held that the Disciplinary Chamber of the Polish Supreme Court is not a tribunal established by law within the meaning of the ECHR (→eucrim 3/2021, 136 and 166).

➤ *Premature termination of judge's mandate violates ECHR*

On 15 March 2022, the ECtHR held – by 16 votes to 1 vote – in the case of *Grzęda v. Poland* (Application no. 43572/18) that there had been a violation of Art. 6 (1) ECHR (right to a fair trial). The case concerned the removal of Judge *Jan Grezda* from the Polish National Council of the Judiciary (NCJ) before his term had ended as well as his inability to obtain judicial review of that decision. Mr *Grzęda* had been elected to the NCJ in 2016 for a four-year term, but his membership was cut short and

ended when new judges were elected to the NCJ by the *Sejm* under an amending legislation in 2018.

The government argued that the lack of access to the courts was not a consequence of the controversial reforms, as NCJ members never had the opportunity (including before the reforms) to challenge the termination of their mandate. While noting that this argument did not even attempt to justify the lack of judicial review in such circumstances, the judges in Strasbourg emphasised that they were fully aware of the weakening of judicial independence and rule-of-law standards brought about by the government's reforms. Grave irregularities included the following:

- The election of judges of the Constitutional Court in December 2015;
- The remodelling of the NCJ;
- The setting up of new chambers of the Supreme Court;
- The extension of the Minister of Justice's control over the courts and his increasing role in matters of judicial discipline.

The ECtHR also referred to its judgments related to the re-organisation of the Polish judicial system, to the relevant CJEU case law, and to rulings of the Supreme Court and Supreme Administrative Court of Poland. It held that only judicial oversight can guarantee judges fundamental protection against the arbitrary exercise of legislative and executive powers; a contrary practice would go against the principle of the rule of law enshrined in all the articles of the Convention and cannot be tolerated, even in respect of procedural rights. The judges in Strasbourg also noted that, as a result of successive reforms, the judiciary has been subjected to interference by the executive and the legislature; its independence has been considerably weakened – the applicant's case is only one example of this general trend.

The Strasbourg judges stressed the importance of the NCJ's mandate to safeguard judicial independence and the link between the integrity of judicial appointments and the requirement of judicial independence. Procedural safeguards similar to those that apply to the dismissal of judges should also be available for the removal of a judicial member of the NCJ from his/her position. The lack of such judicial review particularly impaired Mr *Grzęda*'s right of access to a court – in violation of the ECHR.

Reform of the European Court of Human Rights

ECtHR: Deadline for Applications Reduced to Four Months

From 1 February 2022, the deadline for submitting applications to the ECtHR has been reduced from six to four months from the date of a final decision in a domestic court case. The new deadline can be found in Protocol No 15 to the ECHR, which entered into force on 1 August 2021 (→eucrim 3/2021, 165). The amendment foresaw a transitional period until 1 February 2022; from that date, applications not complying with the new deadline are no longer accepted. As the new time limit is not retroactive, it only concerns applications for which a final domestic decision was issued after 1 February 2022.

Specific Areas of Crime

Corruption

GRECO: Fifth Round Evaluation Report on Greece

On 3 January 2022, GRECO published its fifth round evaluation report on Greece. The on-site visit by the evaluation team took place in June 2021. The focus of this evaluation round is on the effectiveness of the frameworks currently in place to prevent corruption among persons with top executive functions (PTEFs), e.g. ministers, state secretaries, and political advisers as well as members of the police. The evaluation focuses particularly on issues of conflicts of interest, the declaration of assets, and accountability mechanisms (for other reports on this evaluation round →eucrim 1/2021, 40–42 with further references).

Greece has been a member of GRECO since 1999. The country implemented all recommendations in the first evaluation round, 50% in the second round, and 70% in the third round. The compliance procedure for the fourth round on corruption prevention in respect of parliamentarians, judges, and prosecutors is still in progress, with 58% of the recommendations fully, 26% partly, and 16% not implemented so far.

The perception of corruption in Greece remains high, although indicators have shown a gradual improvement in recent years. According to the Corruption Perceptions Index (CPI) published by Transparency International, Greece ranked 59th out of 180 countries in 2020. Its score was 50 (out of a total score of 100, where 0 corresponds to a high level of corruption and 100 to a low level). According to the 2019 special Eurobarometer, 95% of respondents believe that corruption is widespread in Greece (EU average: 71%), 91% have a strong perception of corruption in public institutions (EU average: 70%), and 9% have experienced or seen corruption (EU average: 5%). 58% of the respondents believe that bribery and abuse of power are widespread among politicians, and companies seem rather pessimistic about the criminal justice response to corruption. 81% of respondents believe that bribery is widespread in the healthcare system (EU average: 27%), in line with a recent corruption case that called into question the integrity of several public leaders under investigation for accepting bribes from the Swiss pharmaceutical company Novartis in exchange for patronage.

In 2019, the downgrading of the offence of bribery of public officials from a felony to a misdemeanour, which allowed for more lenient criminal sanctions, was vehemently criticised; the

offence was subsequently reclassified as a felony. Notwithstanding this, GRECO launched an Article 34 procedure on 21 June 2019 – a procedure that can be initiated in exceptional cases where reliable information on institutional reforms, legislative initiatives, or procedural changes indicates a potential serious breach of the CoE's anti-corruption standards. In its *ad hoc r*eport on Greece, GRECO subsequently made four specific recommendations in this respect (→eucrim 4/2019, 248–249). The Rule 34 procedure was terminated on 3 December 2021, following significant improvements to the Greek Penal Code (Law 4855/2021), largely in line with GRECO's recommendations.

Executive power in Greece is shared between the President of the Hellenic Republic (mainly with a representative function) and the government, which is the actual holder of executive power. In this context, GRECO recommends that greater clarity be provided on the status of political advisers (ministerial associates and special advisers); according to the anti-corruption framework that applies to them, they are held to the highest standards of integrity as regards rules of conduct, conflicts of interest, financial disclosure obligations, etc. In addition, for the sake of greater transparency, the names, functions, and any remuneration (for tasks performed for the government) of political advisors, as well as information on potential ancillary activities, is disclosed in a way that provides for easy, appropriate public access online.

The recently modernised internal control and financial disclosure systems are essential tools to prevent corruption of high-level officials at the central level. In addition, the accountability framework for incumbent and former ministers has been significantly strengthened following constitutional amendments in 2019, including immunity provisions. Digitalisation has led to notable improvements in transparency and public consultation mechanisms. Nevertheless, proper implementation of access to information on request remains a challenge. Similarly, further efforts are needed to better ensure meaningful stakeholder involvement at earlier stages of decision-making processes and to monitor external interventions. Following the on-site visit, new lobbying rules were introduced in September 2021 (Law No 4829/2021), the effectiveness of which will need to be proven in practice.

The establishment of the National Transparency Authority (NTA), which has significantly increased cooperation and coordination between the different audit authorities and inspection bodies, marks a milestone in a more holistic approach to anti-corruption policy. The NTA aims to strengthen the national integrity and accountability framework by conducting investigations and audits, developing strategies to prevent and combat corruption, and by raising awareness. The NTA is also responsible for implementing the National Anti-Corruption Action Plan (NACAP), which has been the guiding policy document in the fight against corruption since 2013 – a new version is currently being prepared for the period 2022–2025.

The NTA encourages the development of codes of conduct that are adapted to the nature, challenges, and day-to-day operations of public sector bodies. Pilot projects are underway to establish integrity officers as an institution in individual ministries. At the time of the visit, however, it was not completely clear whether PTEFs would be able to turn to these officers in cases involving ethical dilemmas. Therefore, GRECO suggests further efforts to promote and raise awareness of ethics and integrity issues at the central level.

The supervision of financial disclosure is shared between different institutions, and some initiatives have already been taken in order to streamline methodologies. Nevertheless, more could be done to maximise synergies and to enhance the exchange of information on the best practices of and experience gained by the responsible bodies.

GRECO recommends reviewing the post-employment regime in order to assess its adequacy; the regime could also be strengthened by broadening its scope in respect of PTEFs. The report calls for further streamlining and strengthening of oversight of the declarations of assets and financial interests of PTEFs.

In the area of law enforcement, the report calls for progress in the prevention of police corruption, which was missing in the previous NACAP. Therefore, the NACAP 2022–2025 is to include an anti-corruption regulation for the police, in particular regarding the disciplinary system. The report identifies the working conditions of police officers and effective compensation for overtime as priority areas for improvement. The low proportion of female police officers (14%) is also a major issue, and GRECO calls for dedicated measures to strengthen the representation of women at all levels in the police force.

Although the police have a code of ethics, officers should participate in awareness-raising measures targeted towards their obligations as regards standards of conduct. They should also have access to targeted confidential counselling on ethical and integrity matters.

GRECO recommends updating the code of ethics for the police in order to address current policing challenges. It should include detailed guidance on integrity matters (conflicts of interest, handling of gifts, misuse of information, abuse of public resources, etc.). The professional training measures (initial and in-service) for police officers on ethics are to be further developed, taking into consideration the specificity of their duties and vulnerabilities – with a practice-oriented focus.

A single, realistic, and feasible policy on parallel employment and post-employment may also be necessary, e.g. establishing unequivocal criteria for permissible secondary activities and streamlining the authorisation process to render it clear, timely, and effective. Rules on the employment of police offi-

cers in the private sector after they leave the force also deserve further attention.

The framework for oversight and accountability on the part of the police needs to be strengthened. Further safeguards are necessary to guarantee the objectivity of the investigation and the impartiality of the investigating body and to ensure that they are perceived as such by the public in a sufficiently transparent manner. Lastly, the report calls for all necessary measures to be taken to facilitate the reporting of corruption, including targeted measures to strengthen the protection of whistleblowers within the police by guaranteeing their confidentiality, as appropriate.

Money Laundering

MONEYVAL: Typologies Report on AML/CFT Supervision in Times of Crisis

On 25 January 2022, MONEYVAL published a report that aims to assist authorities in effectively carrying out their supervisory activities as regards anti-money laundering and countering the financing of terrorism (AML/CFT) in times of crisis. The COVID-19 pandemic has created new threats and vulnerabilities to the AML/CFT system. Supervisors have been faced with new challenges, mainly in relation to the proper assessment of risks involved and the communication of appropriate mitigating measures to the obligated entities.

The report is designed as a best-practice paper containing an overview of business continuity measures that supervisors should consider within the context of challenging external factors. It builds on an earlier analysis of AML/CFT trends in MONEYVAL jurisdictions during the COVID crisis (→eucrim 3/2020, 197–198). The report is mainly based on information collected from supervisors of thirty-one MONEYVAL jurisdictions and from other international actors; furthermore, qualitative data were obtained through follow-up interviews and additional written contributions. The questionnaire focused on risks and challenges, solutions to business continuity and crisis management measures, digitalization and other regulatory adjustments as well as supervisory tools, sanctions, outreach, and international cooperation.

The primary challenge for supervision has been the transition to remote working. The pandemic impacted the working conditions of the supervisory authorities by limiting access to buildings and by limiting the number of staff available to carry out daily tasks. In addition to throttled human resources, technical shortcomings (access to IT support, databases, and information from reporting organisations) were also a problem.

Based on a comparison of the different approaches, the report concludes that early business continuity management in the form of Business Continuity Plans (BCPs) has led to minimal disruption to the functioning of supervisory authorities. The majority of the responding supervisors had BCPs for possible crisis scenarios in place before the pandemic outbreak, but only one country's BCP included a specific pandemic scenario. Some jurisdictions had a BCP that had not yet been finalised or not yet adopted, while one jurisdiction reported that its BCP did not cover AML/CFT supervision.

The BCPs include risk assessment methodologies, detailed governance arrangements, division of responsibilities, and specific measures to be implemented in response to a crisis in order to ensure that business can be continued. It has also proven beneficial to include AML/CFT supervision in such plans. Given the physical movement constraints and the need to use virtual meetings and other forms of communication, the involvement of IT and internal security departments in the development of BCPs also appears to be a good practice.

There were new protocols implemented to ensure data security, and staff were trained on related issues. Other measures with positive results included the setting up of coordination committees to distribute AML/CFT supervision among several supervisors.

The pandemic has shown that technology is key in crisis situations in which employees cannot return to the office. In order to mitigate the ML/TF risks, supervisors and data organisations have been encouraged to rapidly increase the digitalisation of their core functions in order to maintain operational continuity. Among other things, video conferencing tools enabled the collection of information/documents from reporting entities on ML/TF risks and hybrid on-site and/or off-site supervision. This is also essential in other challenging circumstances, e.g. monitoring entities with limited or no physical presence in a jurisdiction. Supervisors have also used a variety of communication channels, from posting video clips and e-learning materials to online webinars/training.

The most common IT control measures for remote working across various jurisdictions included the following:

- Using secure VPN connections or joining the call using special platforms;
- Limiting and controlling remote access for users of the institution's server or internal network;
- Restricting downloads from remote computers to personal devices;
- Encrypting locally stored data;
- Recording user activity during remote sessions;
- Multi-factor authentication;
- Regular password changes.

Supervisors have developed guidelines and/or regulations to enable reporting entities to use digital identification systems. Furthermore, they have explored the exceptional use of simplified customer due diligence in low-risk scenarios, for reporting entities to onboard clients and to facilitate the delivery of government benefits.

Cross-border cooperation between supervisors could be enhanced by simplifying existing rules and procedures, including data exchange. Existing mem-

oranda of understanding (MoUs) could include specific provisions for assistance in times of crisis and *force majeure*. In the absence of a specific provision, the general rules of the MoUs could allow and/or encourage communication and cooperation by electronic means, where available.

MONEYVAL member states and territories will be invited to provide feedback on the use and added value of the findings in one year.

MONEYVAL: Fifth Round Evaluation Report on Poland

On 1 February 2022, MONEYVAL published its fifth round evaluation report on Poland. Moneyval called on the Polish authorities to improve the regulatory framework and to strengthen the practical application of measures to stop money laundering and the financing of terrorism (ML/TF). According to the report, most legal requirements and practical actions put in place by the authorities ensure a satisfactory level of transparency of legal persons and beneficial ownership. The report acknowledges that the private sector demonstrates a substantial level of effectiveness in applying ML/TF preventive measures, including customer due diligence and internal controls.

However, Polish authorities have a limited understanding of ML threats emanating from certain types of predicate offences, and they lack a comprehensive view of the factual/detected and potential/undetected amounts of the proceeds of crime. Therefore, further improvements are needed to enhance the country's capacity to understand ML threats, and significant additional efforts are needed as regards appropriate identification and reliable assessment of TF risks.

Poland has a broad range of law enforcement agencies (LEAs), but none of them are designated with specific responsibility to investigate ML. While the Polish Financial Intelligence Unit (FIU) has full access to a wide variety of information from the private and public sectors, the results of its analysis are insufficiently exploited at the investigative stage. Overall, the ML cases are not fully prioritised, and the number of ML investigations lags behind the number of convictions for offences generating proceeds. Therefore, the rate of transforming FIU notifications (and other information sent to the prosecution service/LEAs) into investigations and into corresponding indictments is low. LEAs mainly use the communications for their own statutory activities, with little or no focus on tracing proceeds of crime. MONEYVAL therefore encourages Poland to take procedural and institutional measures to ensure that ML is detected and investigated efficiently. This should include adopting a coherent practice of tasking LEAs with ML investigations as well as detailed guidelines on effective parallel financial investigations.

MONEYVAL calls for fundamental improvements regarding the seizing and confiscating of proceeds of crime from ML and associated predicate offences. The confiscation of proceeds and instrumentalities is not consistent with ML/TF risks, and national AML/CFT policies are not being pursued as a policy objective. Relevant statistics on confiscations applied in relation to predicate offences are lacking, which negatively impacts the authorities' ability to assess the effectiveness of the system and to take targeted policy measures to address any weaknesses. In detected cases of false declaration or non-declaration, the restrained assets concern only the equivalent value of the fine for a fiscal crime and the remaining assets are returned, even in cases of suspicion of ML.

TF cases are conducted primarily in connection with a terrorist offence. In the past seven years, three of several TF cases ended with charges and two TF convictions of four individuals were achieved, which is partially reflects the country's risk profile. However, the sanctions applied were minimal, hence neither dissuasive nor proportionate. Moreover, the prosecution services and other LEAs had not adopted methodological guidelines or instructions for TF investigations and it cannot be concluded that TF investigations have been integrated into and used to support national counter-terrorism strategies.

Moneyval calls on the Polish authorities to take measures to clarify that TF is a stand-alone crime and not a byproduct of terrorism. The cash control mechanisms at the border should be strengthened by providing a legal basis to stop and restrain suspicious assets. A specific risk assessment on the non-profit organisation sector's exposure to TF risks should also be conducted, and targeted measures should be applied for entities that are more vulnerable to TF abuse.

The report recommends that a supervisory system, including a sanctioning regime, on proliferation financing must urgently be put in place. There should be more awareness-raising activities to enhance knowledge and understanding on the part of many authorities and entities in the private sector as to their respective obligations.

Poland has a comprehensive legal framework for international co-operation. It is carried out together with other EU Member States, based on a simplified mechanism; however, co-operation with non-EU jurisdictions is less constructive. The case management system is fragmented, and no guidelines exist with regard to the handling and prioritisation of MLA requests. Although there are no systematic statistics on MLA, extradition, and other forms of co-operation, several successful examples of co-operation in ML and TF cases, including the establishment of JITs, exist. Co-operation in relation to seizing, freezing, confiscating, and sharing of assets is still of limited effectiveness. Although proactive information exchanges with foreign counterparts take place, the extent to which this co-operation is carried out for AML/CFT purposes remains unclear. Except for the FIU, no other supervisory authority exchanges information with its foreign counterparts for AML/CFT pur-

poses, perhaps hampered by such co-operation requiring the prior consent of the Polish Prime Minister, which may well impact the effectiveness and constructiveness of the requested international assistance, especially in urgent cases.

MONEYVAL: Fifth Round Evaluation Report on Croatia

On 3 February 2022, Moneyval published its fifth round evaluation report on Croatia. The understanding of ML risks is uneven between Croatian authorities, ranging from full understanding (Croatian National Bank) to inadequate understanding (tax administration). The understanding of TF risks is poor across all authorities. This disparity is influenced by several weaknesses in the identification and assessment of risks, such as the fact that policy objectives in the area of TF were developed in strategy documents that did not provide information on ML and TF risks. At the operational level, the competent authorities have exhibited good cooperation and coordination on ML/TF issues, but support at policy level is not sufficient in terms of strategic coordination.

Although the Croatian legislation provides the law enforcement authorities (LEAs) with broad powers to identify and investigate ML, investigations mainly focus on the predicate offence, as judges and, to some extent, prosecutors have a limited understanding of ML offences. Competent authorities have access to a wide variety of sources of financial intelligence information, but LEAs use it mainly to obtain evidence and to trace the proceeds of crime related to associated predicate offences. The information is rarely used in the context of ML investigations and never used for TF investigations.

Overall, progress in ML convictions is not in line with the country's risk profile: The ratio between disseminated cases and launched investigations remains low; criminal sanctions applied to ML offences have been neither effective nor dissuasive enough so far.

The Croatian authorities have the legal powers at their disposal to detect, seize, and confiscate instrumentalities, proceeds of crime, and equivalent property. Although there is no high-level policy document governing this area, the measures taken show that confiscation is considered a policy objective to some extent.

While Croatia has confiscated significant proceeds in conjunction with domestic predicate offences, confiscations related to ML have not yielded tangible results. The confiscation results are also not always in line with the country's risk profiles, as described in the 2016 and 2020 national risk assessments.

The Croatian authorities are not sufficiently aware of the TF phenomenon and how different legal and illegal activities can be used for these purposes. Despite some inquiries, no formal criminal or parallel financial investigations have been carried out so far, and thus no prosecutions and convictions for TF offences have been carried out.

Regarding non-profit organisations (NPOs), two national risk assessments were carried out in 2016 and 2020, without identifying the subset of NPOs that fall under the FATF definition and are likely to be exposed to the risk of TF abuse. This has affected the implementation of targeted measures against non-profit organisations.

Information on the creation and types of legal entities and arrangements is publicly available. The Croatian authorities seem to have some understanding of the vulnerability of legal persons and arrangements in the context of ML, but not in that of TF. They focus primarily on criminal schemes and conduct and are reluctant to identify certain types of legal entities as the most vulnerable instruments for ML, despite the fact that most abuse involves limited liability companies.

Measures to mitigate the misuse of legal persons and arrangements do exist (such as different registers, the involvement of a notary in the registration procedure, etc.), but they have weaknesses; sanctions are not systematically applied.

As regards cooperation, Croatia provides constructive mutual legal assistance and extradition assistance in cases of ML/TF and predicate offences (except for fiscal offences when dealing with non–EU Member States). There is, however, no mechanism for prioritising incoming requests in place, and Croatia is seeking foreign co-operation only to a limited extent, which is not in line with its risk profile. Informal cooperation is one strength of the system, but the country lacks a systematic approach to identifying and addressing the underlying systemic problems related to the refusal of extradition requests from foreign partners.

Articles

Articles / Aufsätze

Fil Rouge

The present issue focuses on issues related to the monitoring of money laundering and financing of terrorism, which has become increasingly important in preventing and combatting organised crime and terrorist offences. "Chasing the money" is the strategy to be followed, but indepth analysis is needed on how this approach should be implemented and which actors should play a key role in pursuit of this aim. Altogether five articles address relevant issues that can be classified into three thematic blocks: different forms of cooperation, the actors involved, and the implications of data retention rules on AML.

The first article by *Ludwiczak* and *Bonzanigo* seeks to explain the way in which the Swiss authorities respond to MLA requests from EU Member States in matters of money laundering. Since Switzerland is one of the world's leading financial centres, it receives numerous requests specifically to obtain information from bank accounts and transaction movements. After analysing the content of foreign requests from the angle of dual criminality, the authors go on to address relevant procedural issues.

In the second contribution, *Vogel* reflects on public-private partnerships (PPPs) for preventing and fighting money laundering. His statements focus on highly relevant questions, e.g. the need to identify in advance the concept, nature, and possible functions of PPPs and the need to define the scope and forms of public-private information sharing. He argues that information sharing should be effectiveness-oriented, prioritizing cases that merit closer scrutiny, without losing sight of data protection rights and access to judicial remedies.

Third, *Stulens* analyses the role of local authorities in the prevention of and fight against money laundering. He strongly supports the idea of establishing a more integrated approach towards fighting/preventing organised crime for use by the different branches of local government. The author offers interesting insights into the 2019 EURIEC initiative to promote this type of transnational information sharing.

In the fourth article, *Rubertelli* outlines the role of Italian notaries in the fight against money laundering, highlighting the impact they have in this context, in light of the high percentage of reports on suspicious transactions filed by this group of professionals.

Lastly, *Landerer* explores the widely neglected question of whether the principles defined in the ECJ's case law on data retention of telecommunication data should also be applied to data retention within the AML scheme.

Prof. Dr. Lorena Bachmaier, Universidad Complutense Madrid & eucrim Editorial Board Member

La coopération pénale entre la Suisse et les États membres de l'Union européenne en matière de blanchiment d'argent

Maria Ludwiczak Glassey / Francesca Bonzanigo

In order to fight money laundering, efficient international cooperation in criminal matters is necessary. As Switzerland is one of the world's leading financial centres, it is often approached by foreign states, in particular to obtain bank documents. Switzerland grants extensive judicial cooperation in money laundering matters, provided that foreign requests comply with the requirements of Swiss law on international mutual assistance in criminal matters. The purpose of this contribution is to discuss how the Swiss authorities respond to requests for mutual assistance in money laundering matters submitted by EU Member States. The article does not only give insights into the Swiss law but also into the practice to decide on MLA requests as defined by the Swiss federal courts.

I. Introduction

Pour combattre efficacement le blanchiment d'argent et ses infractions préalables, une forte coopération internationale en matière pénale s'impose. La Suisse détenant une place centrale dans les flux et les activités financières mondiales, elle est souvent sollicitée par les États étrangers, en particulier pour obtenir des pièces bancaires. Afin de garantir l'intégrité de sa place financière, la Suisse accorde une coopération judiciaire large en matière de blanchiment d'argent, ce pour autant que les demandes étrangères respectent les exigences du droit suisse de l'entraide internationale en matière pénale.

Cette contribution se propose d'exposer la manière dont les autorités suisses répondent aux demandes d'entraide judiciaire en matière de blanchiment d'argent provenant des États membres de l'Union européenne. Après une analyse du contenu de la demande étrangère sous l'angle de la double incrimination (II.), nous présenterons quelques aspects procéduraux helvétiques (III.), exposerons l'étendue de la transmission des pièces (IV.) et terminerons par expliquer l'utilisation que peut faire l'État requérant des pièces transmises (V.).

II. Les exigences liées à la double incrimination

Les demandes d'entraide en matière de blanchiment d'argent visent le plus souvent la remise de la documentation bancaire. Or, lorsque l'exécution d'une demande d'entraide implique l'utilisation de mesures de contrainte d'après le droit suisse (*i.e.* en particulier la remise de pièces à conviction, la perquisition, le séquestre ou même la levée du secret), son octroi est subordonné à la réalisation de la condition de la double incrimination (art. 64 al. 1 de la loi fédérale suisse sur l'entraide internationale en matière pénale (EIMP) *cum* art. 5 par. 1 let. a de la Convention européenne d'entraide judiciaire (CEEJ) et la déclaration y relative de la Suisse ; art. 18 par. 1 let. f de la Convention européenne relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime, CBl). La Suisse n'accordera ainsi l'entraide que si les faits fondant la demande sont constitutifs d'une infraction pénale aussi bien d'après le droit de l'État requérant que d'après le droit suisse.

En vertu de l'obligation de motivation résultant de l'art. 14 CEEJ, il appartient à l'autorité requérante d'exposer les faits de manière suffisamment complète pour permettre aux autorités suisses de se déterminer sur la réalisation de cette condition. L'autorité requérante n'a pas à apporter de preuve concrète des faits qu'elle avance, mais elle doit veiller à ce que sa demande ne contienne aucune contradiction ou erreur manifestes.[1] Lui sera par ailleurs accordée la possibilité de compléter sa demande si celle-ci devait se révéler incomplète.[2]

De manière générale, en examinant la double incrimination, les autorités suisses ne procèderont en pratique pas à un examen du droit étranger ; si l'État requérant estime que les faits sont constitutifs d'une infraction d'après son droit, elles partiront du principe que tel est bien le cas, en application des principes de la confiance et de la bonne foi internationales.[3] Les autorités suisses se limiteront donc à s'assurer que les faits exposés dans la demande correspondent aux éléments constitutifs d'une infraction réprimée par le droit suisse, susceptible de donner lieu à la coopération internationale.[4]

Il n'est pas nécessaire que les faits revêtent la même qualification juridique, qu'ils soient soumis aux mêmes conditions de punissabilité, qu'ils soient passibles des mêmes peines, ou encore que les conditions particulières en matière de culpabilité et de répression soient réalisées.[5] La survenance de la prescription n'est pas non plus un élément propre à l'examen de la double incrimination.[6] Il s'ensuit que la demande sera rejetée uniquement si l'on ne parvient pas à attribuer les faits à une infraction du droit suisse, ou encore si la demande porte sur des faits pour lesquels l'entraide est exclue (art. 2 let. a CEEJ *cum* art. 3 EIMP). En particulier, les autorités suisses n'entreront généralement[7] pas en matière sur les demandes portant sur des infractions de nature fiscale, à l'exception de l'escroquerie fiscale (art. 3 al. 3 let. a EIMP)[8] qui, contrairement au simple délit fiscal, implique l'usage de faux.

L'infraction de blanchiment d'argent a la particularité d'être liée à la réalisation d'une infraction préalable qui, en droit suisse, devra être un crime ou une infraction fiscale qualifiée (art. 305bis ch. 1 du Code pénal suisse, CPS). Si l'Etat requérant a connaissance de cette infraction principale, il devra la mentionner dans sa demande et, lors de l'analyse de la double incrimination, l'autorité suisse vérifiera que celle-ci constitue bien un crime ou un délit fiscal qualifié au sens du droit suisse.[9] Le crime est défini à l'art. 10 al. 2 CPS[10] comme une infraction passible d'une peine privative de liberté de plus de trois ans. Par conséquent, ce n'est que si l'infraction préalable retenue est passible d'une telle peine que la Suisse coopérera en matière de blanchiment d'argent. Lorsque l'Accord de coopération entre la Communauté européenne et ses États membres, d'une part, et la Confédération suisse, d'autre part, pour lutter contre la fraude et toute autre activité illégale portant atteinte à leurs intérêts financiers (AAF) trouve application, ce seuil de coopération est allégé, l'art. 2 § 3 AAF prévoyant que l'Accord s'applique également au blanchiment du produit des activités couvertes pour autant qu'elles soient punissables selon le droit des deux parties d'une peine privative de liberté ou d'une mesure de sûreté restreignant la liberté d'un maximum de plus de six mois.

Pour ce qui est du délit fiscal qualifié, il s'agit d'une notion propre à la disposition sur le blanchiment d'argent, définie à l'art. 305bis ch. 1bis CPS. Les infractions de nature fiscale mentionnées dans cette disposition demeurent des formes d'escroquerie fiscale et n'élargissent donc théoriquement pas la coopération accordée par la Suisse dans le domaine fiscal.[11] Cependant, d'après la pratique du Tribunal pénal fédéral suisse (TPF), la double incrimination en matière de délit fiscal qualifié préalable au blanchiment d'argent est interprétée largement.[12] Dans une affaire d'entraide avec le Canada, le TPF a en effet considéré que des « auto-prêts » ayant soustrait au fisc canadien un montant de plus de CAD 12'000'000.– (dépassant les CHF 300'000.– requis à l'art. 305bis ch. 1bis CPS) constituaient un délit préalable au blanchiment d'argent sous la forme du délit fiscal qualifié, sans examiner de manière approfondie si des faux avaient effectivement été utilisés.[13]

Si l'État requérant ignore en revanche la qualification de l'infraction principale mais suspecte uniquement l'origine délictueuse des fonds, sa demande pourra être admise si l'exposé des faits fait état de transactions inhabituelles pouvant objectivement être attribuables à des actes de blanchiment d'argent.[14] Tel sera notamment le cas lorsque les opérations n'ont pas de justification apparente, ou encore lorsqu'auront été effectuées des transactions entre plusieurs sociétés réparties dans différents pays.[15] Ne sera par contre pas suffisante une liste des personnes recherchées et des montants détournés, sans la moindre indication que les comptes sur lesquels la mesure est demandée ont effectivement un lien avec les fonds dont on soupçonne l'origine criminelle.[16]

III. Les aspects procéduraux

1. Réception de la demande et actes d'exécution

Les demandes d'entraide peuvent provenir des États membres de l'UE et, à terme, sans doute également du Parquet européen. Bien que souhaitable, ce n'est toutefois pas possible en l'état. Une révision de l'art. 1 EIMP a eu lieu,[17] permettant sur le principe la coopération avec des entités non étatiques, mais elle doit être complétée par une ordonnance rendue par le pouvoir exécutif. Par ailleurs, l'AAF ne permet selon nous pas la coopération avec le Parquet européen, dans la mesure où il vise à compléter les dispositions de la CEEJ (art. 25 al. 1 AAF), à laquelle l'UE n'est pas partie.[18]

La demande peut être adressée au Ministère suisse de la justice, à savoir l'Office fédéral de la justice (art. 78 al. 1 EIMP) qui la transfèrera à l'autorité d'exécution (art. 79 EIMP), ou directement à l'autorité suisse d'exécution (art. 53 par. 1 de la Convention d'application de l'Accord de Schengen du 19 juin 1990 (CAAS)), pour autant que celle-ci puisse être identifiée. Afin de simplifier la tâche des autorités étrangères, un moteur de recherche ainsi qu'une liste des autorités suisses sont mis à disposition sur le site de l'administration fédérale.[19]

L'autorité d'exécution est en général un ministère public, soit cantonal soit le Ministère public de la Confédération (MPC[20]). La répartition a trait à l'objet de la demande mais aussi à l'existence ou non d'une procédure pénale interne parallèle, l'objectif étant

une bonne administration de la justice et donc l'attribution à l'autorité qui sera en mesure de traiter la demande le plus efficacement, donc aussi le plus rapidement possible.

Une fois la demande en mains de l'autorité d'exécution, celle-ci procède à une brève analyse afin de déterminer si elle est complète ou s'il est nécessaire de requérir des compléments de la part de l'État requérant (art. 80*o* EIMP). Lorsque la demande porte sur des informations bancaires, l'exécution impliquera de s'adresser à la banque et requérir, au moyen d'un ordre de dépôt (art. 265 du Code de procédure pénale suisse), la remise de la documentation en question. La requête sera toutefois, généralement, plus large que ce qui ressort expressément de la demande. En pratique, lorsque l'autorité requérante indique s'intéresser à un virement intervenu sur le compte n° 1 à la banque A. en Suisse, l'ordre de dépôt visera en principe la documentation bancaire complète (*i.e.* y compris les documents d'ouverture – formulaire indiquant le nom de l'ayant droit économique compris – et, cas échéant, de clôture) du compte n° 1. Sera aussi demandée la documentation complète relative à tous les comptes ouverts au nom du titulaire du compte n° 1, dont il est l'ayant droit économique ou sur lesquels il dispose d'un droit de signature.

L'ordre de dépôt adressé à la banque peut être, et est en général, assorti d'une injonction de garder le secret (art. 80*n a contrario* EIMP ; art. 292 CPS) sur la procédure d'entraide en cours. La banque a ainsi, à ce stade, l'interdiction d'informer son client que la documentation bancaire a été transmise.

La documentation bancaire peut également être obtenue lors d'une perquisition dans des locaux, par exemple d'une fiduciaire. La perquisition peut, mais ne doit pas nécessairement être sollicitée dans la demande d'entraide, l'autorité d'exécution suisse pouvant choisir les actes à entreprendre pour fournir à l'État requérant les résultats demandés.

À réception de la documentation, l'autorité d'exécution procède à une analyse, qui peut la conduire à solliciter la banque A. à nouveau ou encore procéder à d'autres actes complémentaires, même si ceux-ci ne sont pas demandés par l'État requérant. Par exemple, des mouvements de fonds peuvent être intervenus vers et depuis des comptes bancaires de tiers, auprès de la banque A. ou d'autres banques en Suisse, auquel cas la documentation bancaire relative à ces comptes peut être demandée à la banque concernée.

Si des fonds sont présents sur les différents comptes identifiés, l'autorité d'exécution peut, de plus, en requérir le blocage provisoire (art. 18 al. 2 EIMP), puis contacter l'autorité requérante afin que celle-ci confirme ou infirme sa volonté de maintenir cette mesure.

2. La clôture de la procédure d'exécution et les voies de recours

Lorsque toutes les mesures d'exécution ont été prises, l'autorité d'exécution informe la personne concernée[21] de la prochaine clôture de la procédure. En d'autres termes, au plus tard à ce moment, la personne titulaire du compte visé est informée de l'existence de la procédure d'entraide et donc, par voie de conséquence, de la procédure pénale dans l'État requérant. Lorsqu'un État étranger présente une demande d'entraide à la Suisse, il doit anticiper le fait que l'existence de sa procédure pénale sera portée à la connaissance des personnes concernées.

Cela peut conduire à des résultats absurdes, comme l'a démontré la pratique récente. La demande étrangère portait sur la mise sur écoute de raccordements téléphoniques. La mesure a été ordonnée et des résultats intéressants, qui auraient pu permettre à l'autorité étrangère d'anticiper la commission d'une nouvelle infraction, avaient été obtenus. L'autorité d'exécution suisse voulait ainsi transmettre ces résultats à l'autorité requérante, mais à l'évidence immédiatement et sans informer la personne concernée. Le cas a été porté devant les tribunaux suisses, jusqu'à la plus haute juridiction qui a considéré que le droit suisse ne permettait pas, en l'état, de procéder à une telle transmission. Le droit d'être entendu de la personne concernée doit ainsi être respecté dans toute procédure d'entraide initiée à la suite d'une demande étrangère,[22] ce qui démontre l'importance accordée par le droit et la pratique suisses au respect des droits individuels, au détriment parfois d'une coopération internationale efficace.

L'information à la personne concernée a pour but de lui permettre d'exercer son droit constitutionnel d'être entendue (art. 29 al. 2 de la Constitution fédérale suisse ; art. 80*b* EIMP) : elle peut se prononcer tant sur le principe de la transmission que sur l'étendue de celle-ci, un délai lui étant imparti à cette fin. L'autorité d'exécution rend ensuite une décision de clôture ordonnant la transmission de documents bancaires à l'État requérant, dûment motivée. Cette décision peut faire l'objet d'un recours, interjeté dans les 30 jours devant le TPF (art. 37 al. 2 let. a ch. 1 de la loi fédérale sur l'organisation des autorités pénales de la Confédération ; art. 80*e* EIMP). L'arrêt rendu par le TPF peut ensuite être attaqué dans les 10 jours devant le Tribunal fédéral (TF ; art. 84 EIMP), mais le recours n'est recevable que si le cas est considéré par le TF comme « particulièrement important », ce qui est rarement le cas. Il ressort de nos observations et des statistiques que les recours interjetés devant le TPF sont en très grande partie rejetés,[23] alors que ceux adressés au TF sont pour la plupart irrecevables.[24]

La transmission effective des pièces à l'État requérant n'intervient qu'une fois le processus terminé. Celui-ci prend

en général quelques mois, à parfois plusieurs années, en fonction de la difficulté de la cause, des actes sollicités, mais aussi du comportement procédural de la personne concernée : si celle-ci coopère, voire consent à la transmission (art. 80*c* EIMP), le processus sera nécessairement plus court que si elle utilise toutes les voies de recours.

3. Les parties à la procédure

Est partie à la procédure celui qui est « personnellement et directement touché » par la mesure d'entraide et « a un intérêt digne de protection à ce qu'elle soit annulée ou modifiée » (art. 80*h* let. b EIMP)[25]. Dans le cas de pièces bancaires, seul le titulaire du compte – personne physique ou morale – est réputé remplir ces conditions (art. 9*a* let. a de l'ordonnance complétant l'EIMP, OEIMP), à la différence par exemple de l'ayant droit économique,[26] et ce même si le compte a été ouvert au nom d'une société-écran,[27] voire sous un faux nom.[28] La qualité de partie dans la procédure pénale étrangère, notamment celle de prévenu[29] ou de partie civile,[30] n'octroie pas de qualité de partie dans la procédure d'entraide suisse. La banque ne dispose pas de la qualité de partie, à moins qu'il ne s'agisse d'un compte de passage dont elle est titulaire.[31] Les tiers mentionnés dans la documentation ne bénéficient pas non plus de la qualité de partie.[32] Ce ne sera donc que le titulaire du compte bancaire qui sera informé de l'existence de la procédure d'entraide, qui pourra s'exprimer sur la transmission puis recourir contre la décision de clôture.

Si les pièces ont été obtenues lors d'une perquisition, la qualité de partie est accordée au propriétaire ou au locataire du lieu perquisitionné (art. 9*a* let. b OEIMP), en dérogation à la règle exposée ci-dessus. Le critère est alors celui de la maîtrise effective sur les pièces.

L'État requérant n'a pas de droit à l'obtention de l'entraide (art. 1 al. 4 EIMP) et n'est pas partie à la procédure d'entraide en Suisse.[33] Ainsi, si la demande est rejetée, il en sera informé sans pour autant pouvoir s'opposer devant les juridictions suisses compétentes. En revanche, l'Office fédéral de la justice dispose de ladite qualité (art. 80*h* let. a EIMP) et peut s'opposer aux décisions rendues par les autorités d'exécution.

4. Les cas particuliers

Trois cas particuliers permettent aux autorités étrangères d'accéder, en cours de procédure d'entraide, aux documents récoltés en Suisse et doivent être signalés ici : la participation des fonctionnaires étrangers à certains actes d'exécution (1.), la transmission spontanée (2.) et la transmission anticipée (3.).

a) Participation des fonctionnaires étrangers à certains actes d'exécution

La loi suisse permet de faire participer les représentants de l'État étranger à l'exécution des actes d'entraide (art. 65*a* EIMP), par exemple une perquisition, ou encore de consulter le dossier de la procédure. Cette participation peut intervenir sur demande de l'État étranger ou être proposée par l'autorité suisse. Toutefois, la mesure a pour but uniquement de faciliter l'exécution de la demande (les représentants étrangers pourront par exemple désigner les pièces qu'ils souhaitent obtenir) et ne doit pas avoir pour conséquence que les pièces soient transmises en violation de la procédure d'entraide décrite *supra* III.1.-2.[34] Non seulement lesdits représentants ne pourront pas emporter les pièces au terme de leur séjour en Suisse (interdiction de faire des copies ou des photographies), mais ils devront fournir aussi des garanties portant sur la non-utilisation prématurée des informations auxquelles ils auront eu accès.[35]

b) Transmission spontanée

Certains moyens de preuve et informations peuvent être transmis spontanément, c'est-à-dire indépendamment d'une demande étrangère (art. 67*a* EIMP). Le but poursuivi par cette forme d'entraide est d'interpeller l'État étranger sur l'existence d'éléments, en possession des autorités suisses, qui pourraient l'intéresser et l'inviter à formuler une demande d'entraide pour les obtenir.[36] S'agissant d'éléments ressortissant au domaine secret comme c'est le cas des données bancaires, la transmission spontanée est limitée aux informations, à l'exclusion de documents qui pourraient être utilisés comme moyens de preuve dans l'État requérant.[37] Ainsi, les pièces bancaires ne pourront pas être transmises par ce biais mais la jurisprudence considère que l'autorité suisse peut fournir un tableau mentionnant les noms et numéros de comptes concernés.[38]

c) Transmission anticipée

Au vu des lourdeur et lenteur de la procédure suisse d'entraide, en particulier face à l'absurdité de la situation quant aux résultats d'écoutes téléphoniques (*supra* III.2.), un processus de révision portant sur la mise en place d'une forme d'entraide nouvelle (transmission anticipée, nouvel art. 80*d*bis EIMP) a récemment été lancé.[39] Le but est de permettre, exceptionnellement, à l'autorité d'exécution de transmettre les pièces récoltées à l'autorité requérante sans en informer, dans un premier temps, la personne concernée. Tel peut être le cas si l'enquête étrangère serait excessivement difficile sans cette transmission, notamment en raison du risque de collusion, ou parce que la confidentialité de la procédure doit être préservée, ou afin de prévenir un danger grave et imminent.[40]

Cette transmission a lieu moyennant la fourniture de garanties par l'autorité requérante, visant à s'assurer :

- que les pièces seront utilisées uniquement pour les besoins de l'enquête mais non pour requérir une décision finale, par quoi il faut entendre notamment une mise en accusation ;
- que l'autorité étrangère informera l'autorité suisse quand le secret pourra être levé afin que la personne concernée puisse être informée et que la procédure ordinaire d'entraide (exposée *supra* III.1–2.) puisse reprendre en Suisse ;
- que si, au terme de la procédure ordinaire, l'entraide est refusée, les pièces en mains de l'autorité requérante seront détruites.

La portée de la nouvelle disposition initialement envisagée était large et visait toutes infractions, mais au terme du processus législatif qui s'est avéré mouvementé, seules les demandes en lien avec la criminalité organisée ou le terrorisme pourront bénéficier de la transmission anticipée.

IV. L'étendue de la transmission

L'étendue de la transmission en matière de documentation bancaire est régie par le principe de la proportionnalité, concrétisé à l'art. 63 EIMP et abondamment précisé par la jurisprudence. Selon ce principe, il ne s'agit pas, pour l'autorité suisse, de se demander si les renseignements requis sont nécessaires ou simplement utiles à la procédure pénale étrangère. Cette question est en principe laissée à l'appréciation des autorités de poursuite de l'État requérant, puisque l'État requis ne dispose en général pas des moyens qui lui permettraient de se prononcer sur l'opportunité de l'administration des preuves. Il est ainsi de pratique constante de ne refuser la coopération que si les actes requis sont « manifestement sans rapport avec l'infraction poursuivie et impropres à faire progresser l'enquête ».[41]

Par ailleurs, le principe de la proportionnalité interdit à la Suisse d'aller au-delà de la demande qui lui est adressée. Toutefois, il y a lieu de relativiser cette affirmation : la pratique veut que la demande soit interprétée largement, « selon le sens que l'on peut raisonnablement lui donner »,[42] ce afin d'éviter de futures demandes d'entraide complémentaires. Il s'en suit que peuvent être transmis même des documents non mentionnés dans la demande,[43] pour autant qu'ils satisfassent au critère de l'utilité potentielle,[44] *i.e.* qu'il existe un lien de connexité suffisant entre l'état de fait faisant l'objet de l'enquête pénale menée par l'autorité requérante et les documents à transmettre.[45] Afin de permettre à l'autorité requérante de faire la lumière sur le cheminement de fonds d'origine délictueuse, ce qui est particulièrement important en matière de blanchiment d'argent, celle-ci pourra être informée de toutes les transactions opérées aux noms des personnes et des sociétés et par le biais des comptes impliqués dans l'affaire, même sur une période relativement étendue.[46] Le but est également de lui permettre la découverte de faits, y compris ceux dont elle ne soupçonne pas l'existence. La jurisprudence constante autorise une coopération large de la part de l'autorité d'exécution « qui justifie de communiquer tous les éléments qu'elle a réunis, propres à servir l'enquête étrangère, afin d'éclairer dans tous ses aspects les rouages du mécanisme délictueux poursuivi dans l'État requérant ».[47]

Concrètement, si l'autorité requérante explique s'intéresser au virement intervenu le 1er janvier 2021 vers le compte n° 1 ouvert à la banque A., la Suisse pourra lui transmettre la documentation bancaire complète relative au compte n° 1, mais aussi celle relative par exemple aux comptes depuis et vers lesquels des mouvements de fonds importants sont intervenus, voire aux comptes de tiers, tels les membres de la famille de la personne initialement désignée dans la demande.[48]

V. L'usage qui peut être fait des pièces transmises

L'usage que l'État requérant peut faire des pièces transmises est limité par le principe de la spécialité. En droit interne suisse, la règle de la spécialité est prévue à l'art. 67 EIMP qui dispose que « [l]es renseignements et les documents obtenus par voie d'entraide ne peuvent, dans l'État requérant, ni être utilisés aux fins d'investigations ni être produits comme moyens de preuve dans une procédure pénale visant une infraction pour laquelle l'entraide est exclue ». La Suisse a formulé une réserve à l'art. 2 CEEJ reprenant les termes utilisés dans la disposition de l'EIMP, de sorte que l'utilisation par l'État requérant des pièces transmises est restreinte dans cette même mesure lorsque la Convention s'applique. Afin de garantir l'effectivité de cette réserve, les autorités suisses devront attirer l'attention de l'autorité requérante sur ces termes particuliers de la transmission des pièces.[49] La CAAS prévoit une règle similaire à son art. 50 par. 3.

Concrètement, il est interdit à l'État requérant d'utiliser les pièces transmises pour une procédure autre que celle pour laquelle l'entraide a été octroyée initialement. La règle de la spécialité garantit ainsi le respect des conditions d'octroi de l'entraide, en particulier la proportionnalité et la double incrimination ;[50] il serait en effet absurde si le droit suisse posait ces exigences strictes pour l'octroi de l'entraide mais autorisait ensuite l'État requérant à utiliser les pièces à son bon vouloir.[51] Cependant, contrairement à ce qui prévaut en matière d'extradition,[52] le principe de la spécialité est interprété largement en entraide. L'État requérant peut éventuellement utiliser les pièces pour la poursuite d'autres in-

fractions, sans autorisation préalable des autorités suisses, à condition qu'il s'agisse d'infractions pour lesquelles l'entraide aurait été octroyée si elle avait été demandée.[53] Le TF considère en outre qu'une fois les pièces transmises, l'État requérant doit pouvoir en disposer de manière complète, ce qui comprend la poursuite de faits qui seraient non punissables d'après le droit suisse.[54] Il est donc imaginable que les pièces reçues dans le cadre d'une demande d'entraide portant sur le blanchiment d'argent soient utilisées par la suite dans la procédure concernant l'infraction préalable, même si celle-ci serait inconnue du droit suisse. De même, l'État requérant qui reçoit les pièces pour la poursuite d'une infraction de droit commun qui ne serait pas une infraction préalable au blanchiment d'argent d'après le droit suisse, pourrait les utiliser dans le cadre d'une telle procédure.[55]

Demeure en revanche une interdiction absolue d'utiliser les pièces reçues dans le cadre de la poursuite d'infractions de nature fiscale, étant donné que la Suisse n'accorde pas de coopération dans ce domaine. Il est de ce fait également interdit à l'État requérant de transmettre les pièces reçues à ses autorités fiscales, et ce même si sa loi interne prévoit une communication large entre ses différentes autorités.[56] En matière d'escroquerie fiscale, l'on exigera de l'État requérant qu'il s'enquiert auprès des autorités suisses sur la possibilité d'utiliser les pièces transmises pour une telle procédure. En effet la distinction entre escroquerie fiscale et délit fiscal simple est délicate et peu connue en dehors de la Suisse, ce qui justifie un certain contrôle préalable.[57]

L'État requérant ne pourra transmettre les pièces reçues à un État tiers qu'avec le consentement des autorités helvétiques.[58]

Dans la mesure où le principe de la confiance régit les relations entre la Suisse et les États avec lesquels elle a conclu un traité d'entraide – ce qui inclut tous les États membres de l'Union européenne – une déclaration expresse sur le respect du principe de la spécialité ne sera pas nécessairement requise ; l'on partira en effet du principe que l'État requérant respecte ses engagements internationaux.[59] L'octroi de l'entraide pourrait par contre dépendre d'une telle déclaration si des violations répétées du principe de la spécialité sont constatées.[60]

VI. Conclusion

La coopération internationale en matière pénale accordée par la Suisse présente une certaine lenteur. Toutefois, elle est accordée de manière large, conformément à l'exigence posée par l'art. 1 CEEJ. Les pièces fournies à l'autorité requérante dépassent fréquemment ce qui est expressément sollicité dans la demande d'entraide et l'utilisation qui peut en être faite est caractérisée par une grande souplesse.

Il n'est pas rare que les demandes d'entraide en matière de blanchiment d'argent conduisent les autorités suisses à ouvrir une procédure pénale, dans la conduite de laquelle elles solliciteront, à leur tour, les autorités étrangères. L'écueil que les autorités suisses doivent éviter alors réside dans la fourniture spontanée, dans une demande d'entraide « retour », des éléments qui auraient dû faire l'objet d'une procédure d'entraide en Suisse. En effet, un tel procédé serait contraire aux règles suisses applicables en matière d'entraide exposées dans la présente contribution, règles qui sont applicables en tout temps, même lorsque les deux États conduisent des procédures pénales parallèles pour des faits connexes.

Maria Ludwiczak Glassey
Prof. Dr. iur., Chargée de cours au Département de droit pénal, Faculté de droit de l'Université deGenève ; Chargée d'enseignement à la Faculté de droit de l'Université de Neuchâtel

Francesca Bonzanigo
MLaw, Assistante au Département de droit pénal, Faculté de droit de l'Université de Genève

1 Arrêt du Tribunal fédéral suisse publié au Recueil officiel (ci-après ATF) 117 Ib 64, consid. 5c ; voir aussi arrêt du Tribunal pénal fédéral suisse (ci-après TPF), RR.2019.172, 28 janvier 2020, consid. 4.1 et les références citées. Les arrêts du Tribunal fédéral (ci-après TF) sont disponibles sur le site <https://www.bger.ch/fr/index/juridiction/jurisdiction-inherit-template/jurisdiction-recht.htm>. Ceux du TPF sont accessibles sur le site <https://bstger.weblaw.ch/index.php?method=search>.

2 TF, 1A.333/2005, 20 février 2006, consid. 3.

3 ATF 116 Ib 89, consid. 3c/aa.

4 TPF, RR.2019.3000-301, du 29 juillet 2020, consid. 2.2; ATF 124 II 184, consid. 4b/cc.

5 ATF 124 II 184, consid. 4b/cc.

6 ATF 116 Ib 452, consid. 4 ; S. Heimgartner, in: M.A. Niggli/S. Heimgartner (édit.), *Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ*, Bâle 2015, Art. 64 N 8.

7 Il existe deux exceptions à ce principe : l'art. 50 par. 1 de la Convention d'application de l'Accord de Schengen du 19 juin 1990 (CAAS) prévoyant que l'entraide est accordée en matière de soustraction d'impôts indirects, et l'entraide judiciaire en matière d'impôts indirects résultant de l'application de l'Accord sur la lutte contre la fraude du 26 octobre 2004

(AAF). Voir aussi L. Moreillon, « La coopération judiciaire pénale dans l'Espace Schengen », in : L. Moreillon (édit.), *Aspects pénaux des Accords bilatéraux Suisse/Union européenne*, 2008, p. 470 s.
8 Voir notamment TPF, RR.2020.197, 4 novembre 2020, consid. 3.1.
9 M. Ludwiczak Glassey, *Entraide judiciaire internationale en matière pénale. Précis de droit suisse*, Bâle 2018, N 440 ; TPF 2015 134, consid. 2.4.
10 Voir à ce propos la réserve de la Suisse à l'art. 6 CBI.
11 S. Matthey, « Blanchiment de fraude fiscale : les conséquences des nouveaux articles 305bis ch. 1bis CPS et 14 al. 4 DPA », *Semaine Judiciaire* 2016 II, 296. Voir aussi GAFI, Mesures de lutte contre le blanchiment d'argent et le financement du terrorisme, Suisse, Rapport d'évaluation mutuelle, Décembre 2016, p. 245 disponible sur <https://www.fatf-gafi.org/media/fatf/content/images/mer-suisse-2016.pdf>.
12 Voir à ce propos R. Zimmermann, *La coopération judiciaire internationale en matière pénale*, 5e éd., Berne 2019, N 602.
13 TPF, RR.2016.266, 30 mars 2017, consid. 2.2.3.
14 ATF 129 II 97, consid. 3.3 ; Zimmermann, *op. cit.* (n. 12), N 602.
15 TPF, RR.2017.211, 16 février 2018, consid. 3.2.
16 ATF 130 II 329, consid. 5.1.
17 Elle n'est toutefois pas encore en vigueur, le délai référendaire échéant le 12 avril 2021.
18 M. Ludwiczak Glassey, « La coopération en matière pénale entre le Parquet européen et la Suisse comme État tiers. Futur ou conditionnel ? », (2019) *eucrim*, 205 ss. Dans ce sens aussi S. Gless /T. Wahl, Die Schweiz und das Europäische Strafrecht, in : U. Cassani *et al.*, Chronique de droit pénal suisse dans le domaine international (2018), *Swiss Review of International and European Law* 03/2019, 450 ss.
19 <https://www.elorge.admin.ch/elorge/>.
20 Pour une comparaison structurelle et matérielle entre le MPC suisse et le Parquet européen, voir M. Ludwiczak Glassey /H. Rodriguez-Vigouroux, « Le Parquet européen: un «Ministère public de la Confédération» de l'Union européenne ? », *Pratique juridique actuelle 2019*, 705 ss, disponible sur <https://archive-ouverte.unige.ch/unige:134232>.
21 Sur cette notion, voir *infra* III.3.
22 Un processus de révision a ensuite été lancé, voir *infra* III.4c).
23 Voir TPF, Rapport de gestion 2019, p. 44 disponible sur <https://www.bstger.ch/fr/media/rapporti-di-gestione.html>.
24 Selon nos statistiques pour l'année 2019, seuls 10 % des recours en matière d'entraide pénale interjetés devant le TF ont fait l'objet d'une entrée en matière.
25 En général, voir G. Bomio /D. Glassey, « La qualité pour recourir dans le domaine de l'entraide judiciaire internationale en matière pénale. La quête du juste équilibre entre efficacité et protection des libertés », *Jusletter* 13 décembre 2010 ; M. Dangubic, « Parteistellung und Parteirechte bei der rechtshilfeweisen Herausgabe von Kontoinformationen », *forumpoenale* 02/2018, 112 ss.
26 ATF 122 II 130.
27 TPF 2007 136.
28 ATF 131 II 169.
29 TPF 2007 79.
30 ATF 127 II 104.
31 TPF 2008 172.
32 ATF 122 II 130.
33 ATF 115 Ib 193.
34 Ludwiczak Glassey, *op. cit.* (n. 9), N 523.
35 ATF 128 II 211.
36 En général, voir A. M. Glutz, in: Niggli/Heimgartner, *op. cit.* (n. 6), Art. 67*a* EIMP; A. Haffter, « Internationale Zusammenarbeit in Strafsachen im Spannungsfeld zwischen Denunziation und Verbrechensbekämpfung : Zur Problematik der spontanen Rechtshilfe (Art. 67*a* IRSG) », *Pratique juridique actuelle* 1999, 116 ss ; M. Ludwiczak Glassey, « Dans la jungle de l'entraide internationale en matière pénale », in: S. Garibian/Y. Jeanneret (édit.), *Dodécaphonie pénale. Liber discipulorum en l'honneur du Professeur Robert Roth*, Genève et al. 2017, p. 117 ss, p. 120 s. disponible sur <https://archive-ouverte.unige.ch/unige:101316>; Zimmermann, *op. cit.* (n. 12), N 413 ss.
37 Ludwiczak Glassey, *op. cit.* (n. 36), p. 120 s. Voir aussi M. Harari/C. Corminboeuf Harari, « Entraide internationale en matière pénale et transmission anticipée à l'État requérant », in : A. Eigenmann/C. Poncet/B. Ziegler (édit.), *Mélanges en l'honneur de Claude Rouiller*, Bâle 2016, p. 77 ss, en particulier p. 86 disponible sur <https://harari-avocats.ch/wp-content/uploads/2017/06/Harari.pdf-00585247.pdf>.
38 ATF 139 IV 137.
39 Les différentes étapes peuvent être consultées ici : <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180071>.
40 Sur ces notions, voir M. Ludwiczak Glassey, « La transmission anticipée : l'avenir de l'entraide en matière pénale?>, *Jusletter* 20 avril 2020.
41 ATF 122 II 367.
42 ATF 121 II 241.
43 TPF 2009 161.
44 A ce propos, voir M. Ludwiczak, « La proportionnalité en entraide internationale en matière pénale. Évolution jurisprudentielle>, *Pratique juridique actuelle* 05/2017, p. 608 ss disponible sur <https://archive-ouverte.unige.ch/unige:101998>; Zimmermann, *op. cit. (n. 12), N 717 ss.*
45 ATF 129 II 462.
46 ATF 121 II 241.
47 TPF, RR.2010.173, 13 octobre 2010.
48 TPF, RR.2016.206, 26 mai 2017
49 Zimmermann, *op. cit.* (n. 12), N 809.
50 Sur ces notions, voir *supra* II. et IV.
51 A. Donatsch *et al.*, *Internationale Rechtshilfe unter Einbezug der Amtshilfe im Steuerrecht*, 2e éd., Genève/Zurich/Bâle 2015, p. 116.
52 Sur le principe de la spécialité en matière d'extradition, voir art. 38 EIMP et art. 14 de la Convention européenne d'extradition (CEExtr). Pour plus de détails, voir R. Garré, in : Niggli/Heimgartner, *op. cit.* (n. 6), Art. 38 N 2 ss .
53 Donatsch *et al.*, *op. cit.* (n. 51), p. 120 ; voir aussi art. 67 al. 2 let. a EIMP.
54 TF, 1C _138/2007, 17 juillet 2007, consid. 2.3.2. Cette conception large de la spécialité est cependant critiquée en doctrine, voir en particulier G. Fiolka, in : Niggli/Heimgartner, *op. cit.* (n. 6), Art. 67 N 10 ss et N 30 .
55 Dans ce sens pour les infractions de nature fiscale pour lesquelles la Suisse coopère mais qui ne sont pas pour autant des infractions préalables au blanchiment d'argent d'après le droit Suisse, L. Unseld, *Internationale Rechtshilfe im Steuerrecht, Akzessorische Rechtshilfe, Auslieferung und Vollstreckungshilfe bei Fiskaldelikten*, Zurich 2011, p. 167 s.
56 TF, 1A.161/2000, 15 juin 2000, consid. 4.
57 Zimmermann, *op. cit.* (n. 12), N 809.
58 Voir notamment TPF, RR.2009.213, 5 octobre 2009, consid. 2.
59 ATF 115 Ib 373, consid. 8.
60 TF, 1A.161/2000, 15 juin 2000, consid. 4g).

Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing

Benjamin Vogel*

In its 2020 Action Plan to comprehensively reform the EU's Anti-Money Laundering and Terrorism Financing (AML/CFT) framework, the European Commission announced, inter alia, that it would issue guidance for Public-Private Partnerships (PPPs). Furthermore, in respect of the envisaged new EU-level Anti-Money Laundering Authority (AMLA), the legislative package published in July 2021 entails a draft provision to allow the AMLA to participate in national or supranational PPPs. If adopted, AML/CFT PPPs will have a legislative foundation in EU law. Though details would still be left to Member States, it is high time to assess the policy ideas behind PPPs as well as their legal ramifications.

I. Public-Private Information Sharing in the Current AML/CFT Framework

The global Anti-Money Laundering and Terrorism Financing (AML/CFT) framework was originally conceived as a system in which the private sector would autonomously screen its customer relationships in order to detect cases where assets are related to criminal activity or where there is at least a suspicion to this effect. Over time, however, there has been increasing awareness on the part of the Financial Action Task Force (FATF) and in the European Union (EU) of the fact that the detection of relevant risks is usually far from being a straightforward task, given that the private sector usually lacks criminalistic expertise and detailed information pertaining to the nature and modi operandi of criminal actors. As a result of these practical limits, the AML/CFT framework has increasingly emphasised the role of the public sector in providing obliged entities with guidance. In the EU, Directive 2015/849 now provides for an obligation on the part of the Commission, the European Supervisory Authorities (ESAs), and Member States to identify and assess money laundering and terrorism financing risks at regular intervals and to make their findings available to obliged entities.1 Further guidance specifying risk factors is required from the European Banking Authority (EBA),[2] and Member States' authorities must provide obliged entities with information on the practices of money launderers and financers of terrorism.[3] EU law, however, specifies neither the scope of such information nor the functioning of the associated information gateways. Moreover, although Financial Intelligence Units (FIUs) are under a general obligation to provide feedback to obliged entities on Suspicious Activities Reports (SARs) filed by the latter,[4] EU law remains silent on the scope and frequency of this feedback. As a result, obliged entities at the level of the Member States have in most cases not received specific guidance beyond the EBA's risk factors[5] and the typologies provided by various supranational institutions, most importantly the FATF.[6] In short, while EU law in the meantime presupposes that public-private information sharing is a prerequisite for the effective functioning of the AML/CFT system, it does not yet provide meaningful guidance on how to put such information sharing into practice. Against this background, the last few years have seen increasing policy debates on public-private information sharing.[7]

II. Ambiguities of Current Policy Debates

Current policy debates on public-private partnerships (hereinafter: PPPs) usually reflect the need to share strategic and also more targeted information in order to improve the private sector's ability to uncover criminal assets.[8] While this particular conception of the potential utility of PPPs appears to be a common denominator in most stakeholders' understanding of PPPs, the term "PPP", or "publicprivate partnership", is used in various ways and frequently reflects a mixture of rather unspecified goals. It is particularly interesting to note that PPPs are often presented as what essentially constitutes an attempt to improve the effectiveness of criminal investigations. This is especially the case when PPPs are proposed as a mechanism to share information to provide authorities with additional information in support of an ongoing investigation or to identify asyetunknown accomplices.[9] If such practices are labelled as PPPs, this entails some potential for confusion. Using the terminology of AML/CFT to describe and evaluate such ongoing investigation-focused "PPPs" can misrepresent the actual potential of those mechanisms to remedy existing deficits of the AML/CFT framework. In fact, investigation-focused information sharing may ultimately do little more than respond to deficiencies in a particular framework of criminal procedure. If, for example, the sharing of information about suspects in the

context of an ongoing investigation is portrayed as an effort to improve the effectiveness of customer due diligence (CDD), and its success therefore measured by the number of SARs attributable to such sharing, the difference between AML/CFT and criminal procedure is blurred in a rather unhelpful way. For what is then called a "SAR" would in other jurisdictions be the mere response of a private party to a request from an investigative authority. Such terminological nuances matter, because they may create the misleading appearance that the information exchange and the resulting SARs do improve the obliged entities' risk detection capacity. Conversely, other information-sharing practices discussed under the term "PPP" are, in fact, aimed at enhancing the obliged entities' ability to detect hitherto unknown criminals and criminal assets and are therefore genuine ways to improve the quality of CDD and resulting SARs. It is important to keep this ambiguity in mind when discussing a framework for PPPs in AML/CFT, not only because there is otherwise a risk that policy debates will apply the term "PPP" to mechanisms that have rather little to do with improving the quality of CDD, but also because stakeholders might otherwise overlook that some practices at the national level, despite not being called "PPPs", may in essence already provide for the possibility of enhancing public-private information sharing.[10] To identify the need for as well as the practical and legal requirements for such mechanisms, it is therefore necessary to identify the nature and possible functions of PPPs, in more detail, and of public-private information sharing, more generally.

III. The Different Meanings of PPP

The idea of public-private partnerships reflects the idea that the implementation of AML/CFT obligations by private entities and the enforcement of these obligations by supervisory authorities is in practice often – and some will argue most of the time – characterised more by the pursuit of formal compliance with rules than the pursuit of effective prevention and repression of crime.[11] This is because, in order to avoid being sanctioned by supervisory authorities for possible compliance violations,[12] obliged entities will first and foremost strive to show that they undertook reasonable steps to conform with the law. This will all too often push them, in an effort to refute possible supervisory criticism, towards applying CDD in a way that is primarily concerned with creating evidence that they followed the law.[13] Effectiveness, in contrast, is a much more relative criterion, making it ill-suited as a standard against which supervisors can assess the compliance of private obliged entities and likewise ill-suited as a standard that obliged entities themselves can look to in protecting themselves against sanctions. As a result, obliged entities regularly do as much as is necessary, but not much more than that, to show that they did not act carelessly vis-à-vis a particular customer.[14] It will often be much less in the interest of the obliged entity to invest additional efforts to inquire into a problematic customer relationship where such efforts – especially if they do not ultimately lead to the detection of criminal assets – will likely not be valued by regulators. In other words, it is often safer for obliged entities to ensure a mediocre compliance performance – that is, just ticking boxes – than to focus on better outcomes. This is not to say that formal compliance does not also produce useful results in many cases. The idea behind the concept of partnerships, however, is that current frameworks could be improved if it were possible to shape them in a more effectiveness-oriented way.

A partnership approach, as is often hoped, can achieve exactly this by ensuring that AML/CFT compliance is able to prioritise cases that merit greater scrutiny. By introducing mechanisms that allow for more dialogue among obliged entities, supervisors, and other competent authorities, a partnership approach can facilitate the discussion of compliance efforts and the pursuit of ways to refine them – all in the spirit of an effective detection of criminal assets. As the term "partnership" implies, such a dialogue requires that both sides be prepared to contribute to the common cause. On the private side, a partnership approach principally presupposes that an obliged entity is willing to go beyond the regulatory minimum and thus demonstrate a commitment not only to its formal compliance with the applicable obligations but also to greater effectiveness. On the public side, partnership entails a willingness on the part of the relevant authorities to listen and respond in an appropriate way to the concerns and difficulties expressed by obliged entities regarding their implementation of compliance obligations and – crucially – regarding the provision of information that may help them overcome or mitigate such difficulties. While AML/CTF PPPs are thus firmly grounded on a legal reality – namely, on the private sector's compliance obligations – the idea of PPPs also constitutes an acknowledgment of the practical limits of top-down command-and-control approaches to regulation. This acknowledgement is evident from one of the primary aims of PPPs: the stimulation and encouragement of a sense of common purpose, based on shared interests of the public and private partners.

AML/CFT consists of a plurality of different key elements ranging from CDD and SARs to FIU analyses and, ultimately, where applicable, criminal investigations.[15] It follows that there are various stages at which closer public-private collaborations may come into play. Although public-private information sharing is the common denominator of PPPs, it is necessary to distinguish precisely how such information sharing is meant to contribute to greater effectiveness – that is, to define the intended purposes of PPPs. Without such differentiation,

any policy debate risks losing orientation and ultimately suffering the fate of all disoriented policy initiatives: a situation in which the resulting measures offer no added value or even worsen the status quo by adding confusion and wasting valuable resources.

Public-private information sharing in the context of AML/CFT may essentially be divided into two primary purposes: the furtherance of ongoing investigations and the improvement of the effectiveness of CDD.[16] Both objectives do, of course, frequently overlap, because more effective CDD is ultimately likely to add value to criminal investigations. However, bearing this distinction in mind is nevertheless vital, because it makes a difference whether the immediate purpose of public-private information sharing is to support the compliance efforts of the private sector or the investigations of competent authorities. To overlook this difference would be to overlook the double purpose of AML/CFT: supporting law enforcement authorities in their investigations into relevant offences and supporting obliged entities in the prevention of ML/TF.

More specifically, each of the two primary purposes of public-private information sharing may again be subdivided into two particular functions that help explain not only the type of information to be shared but also the applicable legal framework and potentially the need for legal reform. As regards the furtherance of ongoing investigations,[17] competent authorities may share information with the private sector to trigger monitoring of the financial conduct of suspects and other persons and entities of interest. This would typically include in particular the sharing of names of targets, and could possibly include the sharing of additional information that may be helpful in rendering the monitoring more effective (for example, information on contact persons or the business activities of the targeted person). Alternatively, competent authorities may provide a private entity with information about persons of interest or profiles of potential suspects, with the aim of allowing the private entity to search its data records in a targeted way.[18] From an operational viewpoint, enabling such targeted searches may be attractive for two reasons. One reason is that it can allow private entities to respond to an information request from an investigative authority without drowning this authority in unstructured and often largely useless bulk data. The other reason is that it may allow investigative authorities to have private data records screened, using offender profiles, for hitherto unidentified suspects.

As regards public-private information sharing with the primary aim of improving obliged entities' CDD,[19] it is helpful to again distinguish between two more specific functions. On the one hand, competent authorities may provide obliged entities with information pertaining to specific SARs, in particular through the provision of feedback once an SAR has been filed.[20] This may entail the provision of information on whether the risk parameters applied in certain cases were appropriate in the eyes of the relevant authority (in particular the supervisory authority or the FIU). The information that competent authorities share with regard to specific SARs may, however, also encompass more personalised data. For example, a competent authority may communicate to an obliged entity that a transaction or customer mentioned in a particular SAR is, according to the assessment of the authority, indeed linked to crime, or that there is reasonable suspicion to this effect. On the other hand, compliance-focused public-private data sharing may entail the provision of information independently of any particular SAR, with the aim of enabling the obliged entity to improve its risk detection capacity. This may, for example, include strategic information about criminal phenomena in a certain region or business sector but also more specific information such as profiles of relevant offenders or even information about particular suspects and their activities.[21]

Lastly, concepts for PPPs cannot and should not be disconnected from broader reflections about legal reform. As already mentioned, the concept of partnership seeks effectiveness by building on the shared interests of the parties in order to encourage both sides to go beyond legal obligations. Voluntariness is therefore a defining feature of PPPs. Insofar as PPPs are a response to deficiencies in the current state of the law or its implementation, however, they ultimately invite reform that goes well beyond the mere establishment of rules for new informal and voluntary mechanisms that would operate as an addition to formalised legal frameworks. Obviously, when policymakers acknowledge that informal and voluntary practices are being used or could be used to remedy insufficiencies in the existing legal framework, this usually indicates a need for the legal framework to be improved sooner or later. Such a need is more pressing when the legal order provides only very limited leeway for informal and voluntary mechanisms that operate outside of judicial oversight or comparable independent oversight. The use of the term "partnership" in current policy debates must therefore not distract from the fact that the calls for PPPs ultimately imply, at least in some respect, a call to reform some rights and obligations of obliged entities. Awareness of this fact is all the more important on the eve of a fundamental reform of the EU AML/CFT architecture[22] that will provide the opportunity to address some of the deficits that underlie calls for PPPs. From this vantage point, developing a framework for PPPs is not only about creating mechanisms that operate as an addition to other elements of the current architecture. Rather, it is ultimately also about adapting current laws towards a more effectiveness-driven implementation of CDD obligations. Similar considerations apply to the other prima-

ry role of publicprivate information sharing – namely, that of supporting ongoing investigations. The role of public-private information sharing in ongoing investigations highlights in particular a number of unresolved questions concerning the relationship between the laws of criminal procedure and AML/CFT laws. Where informal practices of public-private information sharing aimed at supporting ongoing criminal investigations are established, this may constitute an example of PPPs operating in parallel and in addition to measures of criminal procedure (i.e. measures such as judicial information requests and production orders addressed to obliged entities). Where PPPs allow FIUs to share information with obliged entities in support of a particular criminal investigation, this underscores with particular clarity the continuing uncertainty – observable in not a few jurisdictions – of the relationship between criminal justice authorities and FIUs[23] as well as the relationship between the formal gathering of evidence and the informal gathering of criminal intelligence.[24] Here again, it is unlikely that informal and voluntary mechanisms will be able to provide a legally sustainable framework for the exchange of information between competent authorities and the private sector.

IV. Policy Considerations

When designing public-private information sharing mechanisms in view of improving obliged entities' ability to detect criminal assets, policymakers should avoid and prevent practices that would ultimately weaken the thoroughness of CDD and the ability of FIUs and supervisory authorities to detect risky business practices and compliance violations. To this end, it should notably be clear that the production of valuable intelligence must never be recognised as a justification or compensation for a deficient compliance framework. Furthermore, insofar as public and private parties engage in dialogue about operational priorities for CDD or a joint determination of red flags, participating agencies must ensure that the priorities and risks thereby determined are in every case based on impartial, publicinterestfocused policy considerations and reflect these agencies' mission and an up-to-date state of knowledge as regards relevant criminal threats. Participating agencies should always seek and value the experiences of the private sector and strive to improve the effectiveness of CDD by including this expertise in their own work and assisting the private side with tailored guidance. At the same time, however, these agencies must ensure that collaboration on a joint development of priorities and risk parameters is not allowed to deflect compliance attention from business areas which, while being commercially attractive and therefore sensitive for private participants, may entail significant ML/TF risks.

As already indicated, the EU AML/CFT framework is characterised by two central objectives: the fight against crime and the protection of the integrity of the financial sector.[25] This widely recognised differentiation has profound implications for the design and functioning of AML/CFT. For while the two objectives overlap and mutually reinforce each other, they are still defined by fundamentally distinct concerns. The "fighting crime" objective is founded on the idea that financial intelligence offers rich opportunities to better detect and prosecute profit-generating criminality. Often summarised by the phrase "follow-the-money", the crimefighting objective of AML/CFT is manifested most clearly in the mission of FIUs to analyse SARs in order to decide whether a particular suspicious activity should be further investigated. Naturally, insofar as policymakers emphasise this component of AML/CFT,[26] the quality of SAR filing is taken to be of particular importance.

In turn, insofar as policymakers emphasise the other central objective of the AML/CFT framework – namely, the protection of the integrity of the financial sector[27] – somewhat different considerations become important. The "integrity" objective reflects the conviction that it is, for multiple reasons, pivotal to prevent an inflow of criminal assets into the financial sector. This approach, in comparison to the "crimefighting" approach, is based less on the idea that financial entities and their customer data may be useful for the detection and investigation of crime; it is based more on the concern that lawful businesses, government institutions, and wider society would be greatly endangered if criminal actors, and in particular organised criminal networks, were allowed to freely spend and invest their illgotten gains.[28] By assigning to financial institutions (and increasingly other types of obliged entities as well) a gatekeeper function that aims to shield the market from criminal assets and from the criminals who may exercise economic and social power through these assets, this objective focuses less on the gathering of financial intelligence. Instead, the goal of protecting the integrity of financial institutions leads AML/CFT policy to focus on the private sector's ability to prevent the inflow of criminal assets and, to this end, to focus in particular on obliged entities' compliance with their preventive duties.

The "fighting crime" and "protecting integrity" objectives of AML/CFT are of course by no means mutually exclusive but rather may ideally strengthen each other. Policymakers must appreciate, however, that solutions that are good for one objective are not necessarily desirable for the other. It is important to remember this in the present context because policy visions for the design of PPPs are frequently characterised by a one-sided focus on financial intelligence that may not be in the interest of the objective of ensuring effective compliance with preventive duties. Three areas are especially relevant in

this regard: First, an intelligence-gathering focus of AML/CFT will usually prioritise the question whether SARs are adding value to criminal investigations and therefore advocate policies that reduce false positives. However, insofar as policymakers emphasise the protection of the integrity of financial institutions as being an objective equal to the goal of gathering valuable intelligence, it is far from obvious that the value of SARs should be measured exclusively based on their utility for criminal proceedings. An approach that elicits a large number of SAR filings may, for example, offer value also insofar as it can provide FIUs with a more detailed picture of potentially risky situations and thereby enhance FIUs' ability to understand individual obliged entities' risk appetite and, as a result, FIUs' ability to identify particularly risky business practices. Second, the two central objectives of AML/CFT will collide if the gathering of valuable intelligence is prioritised over the gatekeeping function of obliged entities. This would obviously be problematic from the viewpoint of an integrity-focused approach because such rewarding or ex post acceptance of high-risk practices would invite more frequent onboarding of such risks. Third, the more that obliged entities' customer due diligence is treated as a system whose primary function is to respond to leads from competent authorities in order to help these authorities gather intelligence, the more this could effectively relieve these entities from their responsibility to search for relevant risks on their own initiative.

The preceding observations are not inconsistent with a more proactive AML/CFT policy in which competent authorities provide the private sector with up-to-date guidance on criminal phenomena and, in some cases, possibly also more targeted information. They do however explain that designing mechanisms of enhanced public-private cooperation requires heightened awareness of any conflicting interests at stake.[29] To this end, it is pivotal to understand that the two above-described objectives of AML/CFT essentially reflect two different and only partially overlapping visions of the role of the private sector in the fight against crime. The first vision – focusing on the production of financial intelligence – conceives AML/CFT as a surveillance instrument of the state. The second – focusing on the gatekeeping role of obliged entities – puts the emphasis on the goal of preventing the inflow of criminal assets into the legal economy. Both visions are of course intimately interlinked, given that the better the intelligence is, the greater the chances will be of detecting criminal assets. Yet, a one-sided emphasis on intelligence-gathering can also jeopardise the effectiveness of private sector prevention. It is therefore important, when examining AML/CFT in general and enhanced public-private cooperation more particularly, not to look at these issues exclusively through the eyes of investigative authorities, who will often be more interested in the gathering of intelligence than in the effectiveness of the regulatory framework. Insofar as public-private sharing is meant to contribute to ongoing investigations, it is, as already mentioned, usually not appropriate to discuss such sharing as a contribution to the effectiveness of AML/CFT compliance.

Finally, policymakers should seek to fully comprehend the actual reasons for ineffectiveness of current AML/CFT practices before deciding about the shape and scope of enhanced publicprivate cooperation. There can of course be little doubt that the current performance of the framework to detect criminal assets is far from satisfactory.[30] However, while it is clear that obliged entities often lack proper guidance to detect criminal assets, one should not hastily dismiss the quality of current private compliance efforts, especially at a time when new technological solutions for the analysis of bulk data signal the potential that this performance may increasingly improve. In addressing the question how to improve the current state of affairs through new forms of public-private cooperation, policymakers should consider, in particular, that failures in the detection of criminal assets are frequently not the result of insufficient compliance efforts on the part of the private sector but rather the result of insufficient performance by, and underlying inadequate resourcing of, public authorities when it comes to the assessment of the information reported by obliged entities.[31] As long as such obstacles on the public side are not remedied, increasing public-private information sharing remains unlikely to improve the detection and prevention of criminals and criminal assets that are hitherto unknown to the authorities.

V. Legal Challenges

In addition to those policy considerations, public-private information sharing in the context of AML/CFT raises a number of legal challenges for which legislators will have to provide appropriate solutions in order to ensure the sustainability of such mechanisms. Three areas deserve particular attention in this regard: data protection law, the impact of information sharing on the de-risking of obliged entities' customers, and the rights of suspects in criminal proceedings.

With regard to data protection law, there is a growing awareness among public and private stakeholders that the processing of personal data within AML/CFT has to date not been sufficiently addressed by legislators at the EU and national levels.[32] With the decline of cash as a means of payment and the ever-growing digitalisation of financial services, financial data provides increasingly detailed information about the personal life and other activities of citizens. At the same time, one must recall that communication between FIUs and obliged entities is shielded by far-reaching tip-off obligations[33] that usually prevent customers from learning about the processing of their

data by obliged entities and FIUs, thereby effectively preventing affected persons from seeking judicial or other remedies to have the reasons, methods, and outcomes of the processing as well as the accuracy of the underlying data reviewed by an independent body. Given that its main purpose is the identification of criminal suspicion and thus the initiation of criminal proceedings, and that it may therefore have a grave impact on targeted persons, the processing of personal data in AML/CFT must be taken to be of considerable gravity. This is all the more so when obliged entities are entitled or even expected to share information with other obliged entities about suspicious transactions, as a suspicion may thereby effectively give rise to the blacklisting of individuals on the basis of a suspicion, even when the suspicion has never been properly verified by the FIU or investigative authorities.[34] Without proper safeguards, public-private information sharing can significantly increase these existing tensions between data protection law and AML/CFT in that it effectively involves state authorities in obliged entities' processing of data.[35] Depending on the scope and purpose of information sharing, authorities may then effectively control the processing of obliged entities' data records, thereby escalating proportionality concerns.[36] Particular concerns in this regard arise insofar as public-private information sharing is aimed at or results in profiling, thereby categorising individuals in ways that expose them to a heightened risk of being subjected to repressive measures or stigmatised in commercial activities. Such concerns should not be a reason not to develop gateways for information sharing. In fact, greater commitment of competent authorities to obliged entities' AML/CFT compliance may in some respects also offer opportunities to reduce current data protection deficits. PostSAR feedback may, for example, help to ensure that customers do not permanently suffer the consequences of an erroneous risk assessment. However, there can be little doubt that the expansion of AML/CFT through public-private information sharing poses additional challenges to an AML/CFT framework that, already in its current form, frequently struggles to find the right balance between criminal policy needs and data protection law. Defining appropriate rules for public-private information sharing therefore requires prudence to ensure that AML/CFT becomes both more effective and legally sustainable.

Similar to the above-described issues under data protection law, public-private information sharing also highlights questions around existing de-risking practices – that is, the termination of business relationships by obliged entities for the purpose of managing ML/TF risk. To appreciate this point, one must remember that AML/CFT constitutes, among other things, a preventive framework whose enforcement is largely assigned to the private sector. This enforcement takes the form of the requirement that obliged entities abstain from business relationships when they determine that assets are related to criminal activity[37] or when they are unable or unwilling to perform adequate CDD.[38] While the resulting private de-risking practices can sometimes be problematic insofar as they could constitute unlawful discrimination,[39] the current framework benefits from the fact that private entities are, by virtue of their freedom of contract, in principle free not to continue a business relationship with particular customers.[40] By relying on the private sector for ML/TF prevention, legislators thus effectively take advantage of the greater scope of action available to private entities, who are most of the time much less constrained than competent authorities by fundamental rights considerations.[41] This flexibility may however be lost if obliged entities' risk management and de-risking is decisively determined or even just influenced by public-private information sharing. That is, the more that business relationships are terminated or otherwise negatively impacted as a result of information that the obliged entity received from the authorities, the more these consequences will be attributed to the state.[42] In such cases, the lack of meaningful remedies against derisking that prevails under current AML/CFT laws would become particularly difficult to justify. Rules on public-private information sharing could of course anticipate this by prohibiting de-risking on the basis of particular information shared by the authorities. However, such limitations might be much easier to define than to enforce in practice, given that the reasons for the termination of a business relationship will often remain ambiguous. Insofar as public-private information sharing is further developed, legislators may therefore have to give thought to how to improve customers' rights against private preventive measures.

Finally, public-private information sharing can have a profound impact on the relationship between criminal investigations, FIUs, and obliged entities' compliance. Historically, information flows in the AML/CFT framework have in essence been designed as a one-way street through which obliged entities generate financial intelligence that, in suspicious cases, is forwarded to the FIU and then possibly on to criminal justice authorities. This setup, however, is fundamentally changed if information is flowing in both directions, including possibly from criminal investigations to FIUs and to obliged entities. If information is allowed to flow in both directions, FIUs' operational analysis and obliged entities' CDD could effectively be transformed into a surveillance and intelligence gathering framework that may be triggered by information generated in criminal proceedings[43] and may ultimately serve those proceedings but will at the same time, in principle, not operate under the rules of criminal procedure law. Insofar as this leads to the gathering outside of criminal proceedings of information for the furtherance of criminal proceedings that are already ongoing at the time of the public-private sharing, legislators will need to define the relationship between both legal frameworks and regulate how information obtained with the

help of obliged entities can be used. In particular, insofar as the information generated by obliged entities' CDD can, under the rules of the applicable criminal justice system, be used as evidence, public-private information sharing may result in the circumvention of rights provided to suspects under criminal procedure law. Under such a scenario, affected rights could include, for example, those guaranteeing judicial authorisation or at least judicial oversight of the requisition of documents. One of the attractions of the use of FIUs and CDD as a de facto investigative tool may, in fact, lie in the flexibility of data gathering under AML/CFT laws. Given that AML/CFT is subject to extensive confidentiality obligations, suspects may then, however, be prevented from understanding how particular incriminating evidence was produced. Moreover, insofar as public-private information sharing leads an obliged entity to inquire into a customer's activities, possibly by requesting information directly from the customer, the entity may effectively act as an informant of investigative authorities without its action being subject to judicial or other impartial oversight.[44] Though different national jurisdictions may allow for different degrees of flexibility in this regard, especially the public-private sharing of information regarding particular suspects suggests a need to clarify the respective roles of investigative authorities and FIUs. This would ultimately invite a stronger emphasis on the distinction between evidence-gathering and the gathering of mere criminal intelligence. Not least for the sake of safeguarding defence rights, any sharing of information aimed at supporting ongoing investigations would then naturally fall to investigative authorities. The role of FIUs would then, in turn, be limited to the sharing of information aimed at improving obliged entities' risk management – a division of competences that would also prevent FIUs from getting too intimately involved in criminal investigations and thereby putting the confidentiality of their communication – not least with obliged entities and foreign partners – at risk of being compromised.[45]

VI. Outlook

To summarise, one should recall that the introduction of public-private information sharing mechanisms raises complex questions both as regards the determination of AML/CFT policy and as regards the drafting of an adequate legal framework. It is, to this end, particularly important to clearly differentiate between the function of the AML/CFT framework to protect the financial system from criminal assets and the function of this same framework to support criminal investigations. These two functions must not be confused, because the distinction between them is key for deciding about the design of public-private sharing. In the latter case, such sharing is ultimately about the design of criminal procedure law, while in the former case it is about improving the performance of the regulatory framework. While a public-private information sharing policy must certainly deal with important limitations, especially from data protection law, policymakers will also need to recognise that, in a globalised world, reliance on closer cooperation with the private sector can offer promising opportunities to address today's challenges resulting from transnational organised crime, terrorism, and malign state actors. However, as explained, enhancing the role of public-private sharing will require legislators to address legal deficits of existing AML/CFT laws. Otherwise, public-private sharing could lead to an exacerbation of existing problems that would then sooner or later damage the AML/CFT system instead of improving it.

Dr. Benjamin Vogel
Senior Researcher at the Max Planck Institute for the Study of Crime, Security and Law and leader of the project Public-Private Partnerships on Terrorism Financing (ParTFin)

* Research for this article has been funded by the European Union's Internal Security Fund – Police. The content of this study represents the views of the author only and is his sole responsibility. The article is an amended version of the author's response to the Commission, which was submitted as part of its public consultation on 27 July 2021 to receive guidance on the rules applicable to PPPs within the framework of preventing and fighting money laundering and terrorist financing.

1 Art. 6 paras. 1–3 and 5, Art. 7 paras. 1 and 4(a)(e) of Directive (EU) 2015/849 of 20 May 2015, *O.J.* L 141, 5.6.2015, 73 as amended by Directive (EU) 2018/843 of 30 May 2018, *O.J.* L 156, 19.6.2018, 43.
2 Arts. 17 and 18(4) of Directive (EU) 2015/849, as amended by Directive (EU) 2019/2177, *O.J.* L 334, 27.12.2019, 155.
3 Art. 46 para. 2 of Directive (EU) 2015/849.
4 Art. 46 para. 3 of Directive (EU) 2015/849.
5 European Banking Authority, "Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The ML/TF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849, 1 March 2021, <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf>. All hyperlinks in the endnotes of this article were accessed on 24 March 2022.
6 See for example FATF, Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing of September 2020.

7 For comprehensive accounts, see N. Maxwell and D. Artingstall, "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime", *RUSI Occasional Paper*, 2017, <https://rusi.org/explore-our-research/publications/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime>; N. Maxwell, "Expanding the Capability of Financial Information-Sharing Partnerships", *RUSI, Occasional Paper*, 2019, <https://rusi.org/explore-our-research/publications/occasional-papers/expanding-capability-financial-information-sharing-partnerships>.
8 See already P. Reuter and E. Truman, *Chasing Dirty Money: The Fight against Money Laundering*, 2004, pp. 176–177.
9 For an analysis of tactical information sharing mechanisms, see the categorization in N. Maxwell, "Five years of growth in public–private financial information-sharing partnerships to tackle crime", *Future of Financial Intelligence Sharing (FFIS)*, 2020, p. 13 < https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2020.pdf>.
10 For an example of the sharing by investigative authorities of tactical information for the purpose of identifying offenders, see Bundesverfassungsgericht (BVerfG) [German Federal Constitutional Court], (2009) *Neue Juristische Wochenzeitschrift (NJW*), 1405, 1407.
11 See A. Verhage, "Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry", (2009) 52 *Crime, Law and Social Change,* 29–30; A. Amicelle and V. Iafolla, "Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing", (2018) 58(4*) The British Journal of Criminology*, 855–857.
12 W. Laufer, "Corporate Liability, Risk Shifting, and the Paradox of Compliance", (1999) 52 *Vanderbilt Law Review*, 1402–1404.
13 See N. Ryder, "Is It Time to Reform the Counter-terrorist Financing Reporting Obligations? On the EU and the UK System", (2018) 19 *German Law Journal,* 1185–1186.
14 For a critique of this tick-the-box approach, see European Banking Federation, "Lifting the Spell of Dirty Money: EBF blueprint for an effective EU framework to fight money laundering", *EBF*, 2020, < https://www.ebf.eu/wp-content/uploads/2020/03/EBF-Blueprint-for-an-effective-EU-framework-to-fight-money-laundering-Lifting-the-Spell-of-Dirty-Money-.pdf>, 4.
15 B. Vogel and J. Maillart, "National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection", 2020, <https://pure.mpg.de/rest/items/item_3262446_6/component/file_3286393/content> accessed 24 March 2022, pp. 911–1024.
16 Ibid., pp. 924–925; see also European Data Protection Supervisor (EDPS), "Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing", 23 July 2020 <https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf> para. 38–41.
17 Art. 13 para. 1 s. 1 (d) and Art. 18 para. 2 s. 2 of Directive (EU) 2015/849 of 20 May 2015, as amended by Directive (EU) 2018/843 of 30 May 2018.
18 B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 930–934.
19 Ibid., pp. 1021–1024.
20 See Art. 46 para. 3 of Directive (EU) 2015/849; for the lack of feedback in current practice, see European Commission, "Commission Staff Working Document Impact Assessment accompanying the Anti-money laundering package", SWD(2021) 190 final, p. 12.
21 For a detailed account of the various types of information shared within PPPs for the purpose of improving obliged entities' risk detection, see N. Maxwell, *op. cit.* (n. 9), 26–84.
22 European Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010", COM(2021) 421 final.
23 For a clarification of FIUs' access to law enforcement data, see now European Commission, "Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849", COM(2021/) 423 final, recital 47 and Art. 18 para. 1(c).
24 See B. Vogel (ed.), *Secret Evidence in Criminal Proceedings: Balancing Procedural Fairness and Covert Surveillance*, 2021.
25 See recital 1 of Directive (EU) 2015/849 and recital 1 of Directive (EU) 2018/1673. On the somewhat inconclusive historic origin of the AML framework, see P. van Duyne, H. Harvey and L. Gelemerova, The Critical Handbook of Money Laundering: Policy, Analysis and Myths, 2018, pp. 41–90.
26 See Europol, "From Suspicion to Action, Converting financial intelligence into greater operational impact", *Financial Intelligence Group*, 2017, <https://www.europol.europa.eu/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf accessed 24 March 2022>, 29–30.
27 To this effect European Commission, "Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions", COM(2019) 373 final.
28 See the preamble of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988, United Nations Treaty Series, vol. 1582, p. 95; see also P. van Duyne, "Money laundering policy: fears and facts", in P. van Duyne, K. von Lampe and J. Newell (eds.*), Criminal Finances and Organised Crime in Europe*, 2003, p. 76.
29 For an illustration, see Deloitte/Institute of International Finance, "The global framework for fighting financial crime: Enhancing effectiveness & improving outcomes", *The Institute of International Finance and Deloitte LLP White Paper*, Issue 06/2020, <https://www2.deloitte.com/content/dam/Deloitte/tw/Documents/financial-services/tw-the-global-framework-for-fighting-financial-crime-en.pdf> where the added value of PPPs is explained by the conceptual starting point that "a government's 'victim of crime' is usually a bank's 'customer'. […] both parties, public and private, have an interest and an obligation to work in support of each other in protecting that person and the public more widely". Such a claim can be misleading. For it overlooks that, for the purpose of preventing and detecting money laundering, a bank's customer is first and foremost relevant insofar as s/he is a perpetrator.
30 To this effect already KPMG, "Money Laundering: Review of the Reporting System", *Cja/NCIS web site and report wording*, 2003, <https://www.dematerialisedid.com/PDFs/kpmgreport.pdf>
31 See FATF, "AML/CFT and public-private sector partnership", *FATF*, 2016, <https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-private-sector-partnership.html>, adding that "[i]t has not helped that the governments have lost large numbers of their experts to the banks."
32 See European Commission, "Commission Staff Working Document Impact Assessment accompanying the Anti-money laundering package" SWD(2021) 190 final, pp. 52–55.
33 Art. 39 para. 1 of Directive (EU) 2015/849.
34 See notably EBA, "The ML/TF Risk Factors Guidelines of 1 March 2021", *op. cit.* (n. 5), para. 2.5, which explicitly mentions allegations of criminality against the customer as a potentially relevant risk factor, and further specifies that "[f]irms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing."
35 See also EDPS, "Opinion 5/2020", *op. cit.* (n. 16), para. 41–47.
36 B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 927–928.
37 Art. 35 para. 1 of Directive (EU) 2015/849; Art. 3 para. 1 of Directive (EU) 2018/1673.
38 See Art. 14 para. 4(1) of Directive (EU) 2015/849.
39 See European Data Protection Supervisor (EDPS), "Opinion on a proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds", 4 July 2013, <https://edps.europa.eu/data-protection/our-work/publications/opinions/prevention-money-laundering-and-terrorist-financing_en> para. 78; T. Durner and L. Shetret, "Understanding bank de-risking and

its effect on financial inclusion", *Oxfam*, 2015, <https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf> pp. 9–12.

40 See D. Artingstall, N. Dove, J. Howell and M. Levi, *Drivers & Impacts of Derisking*, 2016, pp. 17–27.

41 But see B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 964–965 on the horizontal effect of the right to non-discrimination.

42 See ECtHR (Grand Chamber), 3 April 2012, *Kotov v. Russia*, Appl. no 54522/00, paras. 102–103.

43 For more on possible covert surveillance of customers as a result of the interplay between FIUs and obliged entities: B. Vogel and J. Maillart, *op. cit.* (n. 15), pp. 904–911 and 923–925.

44 To this effect also EDPS, "Opinion 5/2020", *op. cit.* (n. 16), para. 41–45.

45 B. Vogel and J. Maillart, *op. cit.* (n. 15), p. 943.

The Role of Local Authorities in the Prevention of and Fight against Money Laundering

The Need for More Possibilities for International Information Exchange in the Administrative AML Approach

Gennard Stulens

Criminal organisations use and misuse legal structures in order to launder the money they earn through crimes. Local authorities can unwittingly and unwillingly facilitate crime and money laundering. After all, criminals or people who can be linked to crime and money laundering have to make use of certain legal structures in order to launder their money. They have to apply for permits, they need housing, etc. In order to prevent this misuse of legal structures, the information exchange between law enforcement authorities is necessary, and an administrative, integrated approach to preventing and fighting organised crime is needed. Such information exchange often poses problems in border regions, however, as most of the laws with regard to information exchange between different authorities are written with purely national situations in mind. In border regions, citizens from neighbouring countries often also apply for certain permits if they wish to do business in a municipality. In such cases, obtaining information about these persons is often more difficult because of the lack of (inter)national legislation. Hence, border regions have a greater chance of being misused for money laundering purposes. This article presents and explains the results of a project by the Euro-regional Information and Expertise Centre (EURIEC). The project aims, *inter alia*, to analyse the possibilities and "bottlenecks" with regard to the (cross-border) exchange of data, with a view to enhancing the administrative approach to organised crime.

I. Introduction: The Administrative and Integrated Approach to Combating Organised Crime

Traditionally, the prevention of and fight against organised crime and money laundering is considered a task solely for law enforcement authorities, e.g. the police and prosecutors' offices. This view ignores the fact that local authorities can and should also play a role in the fight against and the prevention of organised crime/money laundering. Additionally, local authorities may also have a lot of information that could provide early signs of organised crime and help prevent and detect it. Public authorities have several instruments at their disposal for preventive and/or reactive action against (organised) crime. The administrative approach involves the use of such instruments.[1]

For, in order to commit certain crimes and launder money, criminals and criminal organisations have to avail themselves of legal structures. Criminal organisations need properties for drug labs or hemp plantations; they need certain businesses to launder the money they earn with the trafficking of drugs, weapons, and even human beings. For some of these business enterprises, like the opening of bars or restaurants, a permit is needed that has to be granted by the local authorities. Before granting this permit, the local authorities collect information from other partners in order to make an informed decision and rule out that this business will be used for criminal activities. In border regions, like the Rhine-Maas region, the necessary information can be provided, for example, by the police and other services within the municipality in Belgium, North Rhine-Westphalia, and the Netherlands. If it is not possible to

obtain such information, criminals or criminal organisations can go about their business undisturbed and launder their money. In such cases, those businesses acting in good faith will have a competitive disadvantage compared to license holders with a criminal background and/or criminal purpose like laundering drug money.

Authorities in Belgium, North Rhine-Westphalia, and the Netherlands are becoming increasingly aware of the fact that a more organised governmental structure is needed to prevent organised crime and money laundering at the local level. Different branches of local government must be able to work together, share information, and have the possibility to form a united front against organised crime. This is why there has been a development from an administrative approach to a more integrated approach for example with the creation of regional information and expertise centres in Belgium and the Netherlands (the ARIECs/PAALCO in Belgium and RIEC-LIEC structure in the Netherlands). These centres advice and support municipalities in the administrative and integrated approach. Within such an integrated approach, different partners like the police, local authorities, the public prosecutors' offices, and tax authorities are brought together to map out which signs of criminal organisations exist and which measures can be taken to stop them.

However, when criminals become aware that the local government in one country is becoming more and more organised, they will try their luck elsewhere, for example in neighbouring countries, where the authorities may have less information about the criminal organisations. This is why an administrative and integrated approach at the international level is urgently needed. This holds especially true for the European Union, due to the freedom of movement and the right of persons to free choice of residence (Art. 3(2) TEU).

II. Towards an International Administrative and Integrated Approach

Honest people make use of the freedom of movement and residence, but so do criminals. When criminal organisations become the focus of the authorities in one of the EU Member States, their members know they can cross the border and try to start over in another Member State. It is possible that criminals cross the border but that information about their organisation or criminal activities does not.

A Dutch mayor, for instance, has the possibility to close down a house pursuant to Art. 13 of the Dutch drug law[2] after a drug lab had been found there. But the owner of the house may also own a bar just across the border in Belgium, where he can launder the money he made through the drug lab. It seems logical that the Dutch mayor would contact the Belgian mayor of the municipality in which the bar is located in order to reveal the activities of the person holding a permit in the Belgian municipality (in this case a permit to serve alcoholic beverages). In reality, this cross-border information exchange is difficult, as national and international legislation in this regard is often lacking. Therefore, a person suspected of operating a drug lab in the Netherlands could still launder drug money in a Belgian bar.

1. The Euregional Information and Expertise Centre (EURIEC)

In order to prevent such situations from occurring, the Belgian Minister of Security and Home Affairs, the Minister of Home Affairs of North Rhine-Westphalia, and the Dutch Minister of Justice and Security signed a declaration of intent in May 2018. They declared their wish to reinforce their collaboration towards improving the information exchange for the purpose of facilitating the administrative approach between Belgium, North Rhine-Westphalia, and the Netherlands. In 2019, the EURIEC (Euregional Information and Expertise Centre) was created as a result of this declaration, funded partly by funds of the European Union's Internal Security Fund.

The EURIEC is an international organisation of Belgium, North Rhine-Westphalia, and the Netherlands, which has a twofold objective:

- Advising municipalities and other partners in cases where there are indications that a person has links with organised crime and where there is a cross-border element. In some of these cases, the EURIEC brings together partners in international expert platforms. In these expert platforms, the possibilities and "bottlenecks" with regard to international information exchange become more and more apparent. When the EURIEC notices that cross-border information exchange is hampered, it contacts the competent authorities and tries to find a mutual solution;
- Raising awareness about the administrative approach and the need for greater international cooperation. National laws are often designed for purely domestic situations, but, in an increasingly global world, international aspects should be also taken into account when drafting/changing legislation.

The EURIEC has assisted Belgian, German, and Dutch municipalities and other partners asking for advice in more than 100 cases with a cross-border element in the past two years. The organisation noticed that some subject matter was recurring in the cases and started writing reports on certain recurring themes, for example: Can a cross-border exchange of police data be carried out for the purpose of the administrative ap-

proach on organised crime? What about financial and judicial data? The following section outlines the possibilities and bottlenecks with regard to the cross-border information exchange of different types of data for the purpose of the administrative approach – as experienced in the EURIEC project.[3]

2. Current possibilities and bottlenecks with regard to international information exchange

a) Overall lack of a national legal basis

A recurring, overarching problem is the lack of national legal bases for the transfer of cross-border information with regards to personal data. A national legal basis is one of the conditions set out by the General Data Protection Regulation for the provision of information. Without such a legal basis, the exchange of information is often impossible, as the protection of personal data and the right to privacy could be affected.

Furthermore, it appears that legislation in Belgium, the Netherlands, and Germany is still based on the view that ensuring public order and security is solely a task of law enforcement bodies (the police and the public prosecutor). The above-mentioned administrative approach is a (relatively) new concept in many countries, which means that legal bases explicitly addressing the exchange of data in this area are often lacking. This problem plays a role not only for data exchange at the international level but often also for the national level, where it is sometimes unclear which information can be shared with other partners for the administrative purposes described above. This lack of a legal basis for both the international and national exchange of information creates legal uncertainty and can lead to a certain amount of caution when it comes to information sharing. In turn, this dilemma plays into the hands of criminals and criminal organisations.

b) Cross-border exchange of administrative data

In contrast to other types of data, e.g. police data, judicial data, and tax data, there is no international regulation on the cross-border exchange of administrative data between local administrations. Additionally, there is often no national legal basis for the exchange of personal data with other (foreign) local authorities. Therefore, and due to the principle of confidentiality, it is generally impossible to exchange personal data between local authorities in Belgium, North Rhine-Westphalia, and the Netherlands.[4]This situation leads to a lack of information exchange about persons and businesses who/which misuse the legal structures. It is, for example, possible that a permit is not granted in one country because of the criminal background of a permit applicant/holder. If the municipality sees that the same person moves his/her activities to another country, the municipality cannot in general, inform the foreign municipality about where he/she restarts his/her business. This creates more opportunities for criminals to launder their money, because all they have to do is cross the border.

c) Cross-border recovery of administrative sanctions and recovery claims

Public (municipal) authorities in Belgium, the Netherlands, and Germany may have claims against persons who are linked to organised crime and possible money laundering, including administrative fines and recovery claims. The possibilities for cross-border collection of restitution claims and administrative fines are often still uncharted territory for most local governments. In practice, it appears that such claims (which are usually and frequently applied in the context of organised crime) are not or only partially recovered when a cross-border component is involved. For instance, recovery often proves difficult when it turns out that the person on whom the sanction was imposed subsequently has moved abroad. In such cases, municipalities will more readily choose to simply write off the fine in their accounts and not collect it. Criminals know this and take advantage of it.

With regard to the cross-border recovery of administrative sanctions and recovery claims, Framework Decision 2005/214/JHA on the application of the principle of mutual recognition to financial penalties,[5] offers cross-border possibilities. This Framework Decision deals only with (administrative) sanctions that are punitive in nature. As a result, administrative fines in Belgium, Germany, and the Netherlands generally fall within the scope of the Framework Decision, but recovery claims, such as the incremental penalty payments which are aimed at restoration do not fall within the scope of the Framework Decision. The reason for this is that the purpose of an incremental penalty payment is, for example, to induce the citizen to undo a violation in whole or in part or to prevent a repetition of a violation. Therefore, recovery claims do not have a punitive nature, cannot be called a sanction and do not fall within the scope of the Framework Decision. In sum, administrative sanctions can in principle be recovered cross-border as the administrative sanctions have a punitive nature and therefore fall within the scope of the Framework Decision. Such an international framework is lacking with regards to recovery claims and therefore the cross-border recovery of such claims is impossible at the moment.

d) Cross-border exchange of police data

In the context of the administrative approach, local authorities often base their decisions on certain police information. If the

person is a foreign citizen, the question arises as to whether it is possible to obtain information from foreign police forces.

None of the treaties or regulations in force that provide possibilities for the exchange of police information contain a provision explicitly providing for the exchange of police data for administrative purposes. The principle of these treaties is the exchange of information between police services for criminal purposes. However, almost all treaties provide for the possibility to transfer police data for purposes other than the (criminal) purposes referred to in the treaties. In order to be able to exchange information for administrative purposes, two conditions have to be met:

- The transmitting authority needs to give its consent;
- This consent must be in accordance with the national law of the transmitting and receiving Member States.

These conditions are rarely met in the national legislations of Belgium, North Rhine-Westphalia, and the Netherlands. This makes the exchange of police information as part of the administrative approach difficult, as the foreign police information cannot be transferred to other partners, such as local authorities. Therefore, the chance always exists that municipalities issue permits to persons who are known to be connected to a criminal organisation in another country. This permit can in turn be used to launder criminal money.

e) Cross-border exchange of financial data

Tax authorities typically have information about the financial situation of individuals and businesses. This information can also be very useful for administrative bodies in the context of tackling organised crime. Financial data can be important because it can reveal, for example, the source of the funding for a certain big real estate project. Such projects can be used to launder criminal money. However, financial data are often subject to a specific confidentiality obligation, which makes the (cross-border) exchange of such data as part of the administrative approach difficult. Such an exchange is not regulated in the most important international legal statutes dealing with exchange of tax information. However, some conventions and agreements allow data provided for the purpose of tax procedures to be used for other purposes as well. For such an exchange of data, similar conditions as those for the exchange of police data apply.[6]

Most national laws in Belgium, Germany and the Netherlands do not provide for a procedure that could serve as a legal basis for consenting to the cross-border exchange of tax data for the administrative approach, meaning that the exchange of such data is rendered impossible. But in some countries like the Netherlands, it is possible to get an overview of the real estate owned by a certain person by consulting (semi-)public sources. This could already give an indication of the financial situation of certain persons.

III. Conclusion

Preventing and fighting organised crime and money laundering is not just the task of law enforcement authorities such as the police and the public prosecutors' offices. Local authorities and other partners can and should also play a role in fighting organised crime and money laundering in the most efficient way. When these partners are not or only insufficiently involved, it is easier for criminals and criminal organisations to launder the money they have earned with their criminal activities. Indeed, in order to launder money, criminal organisations often make use of legal structures, i.e. they have to apply for certain permits, they need housing, etc. To prevent this from happening, local authorities and other partners should make use of the administrative approach against organised crime and act with the instruments that confer corresponding powers (e.g. granting/withdrawal of permits). In order to make use of these powers, information from other partners is necessary. In some purely domestic situations, it is possible for different branches of the (local) government to come together and decide which actions can be undertaken against certain criminal organisations. The criminals are organised, so why shouldn't the government also act in a more organised and integrated manner?

Local authorities and other partners are becoming increasingly aware of their role in the fight against organised crime, and national laws make the information exchange about a country's own citizens possible in certain cases. But when a person applying for a permit is a citizen of a neighbouring country, for example, the information exchange is less self-evident.

This is the reason why the Euregional Information and Expertise Centre (EURIEC) was founded in 2019. On the one hand, the centre aims to raise awareness about the international aspects of the administrative approach and, on the other, it aims to make clear which cross-border sharing of information is permissible, as experienced in practical cases. During the initial years of the project, it became clear that national laws often only take into account the exchange of information in purely national cases. National laws often ignore the international context in which we are living and make an international information exchange impossible. Therefore, local authorities and other partners in border regions are often less informed about the citizens of neighbouring countries, for example when they apply permits. As a result, border regions risk being exploited by criminal organisations that try to launder their money in these regions.

Gennard Stulens LLM & MSc
Public Affairs Officer at the EURIEC,
www.euriec.eu

During the next several years, the EURIEC will meet with legislators in Belgium, Germany, and the Netherlands to make a more efficient administrative and even integrated approach possible. They strive to create a European Union in which authorities are able to work together beyond borders in the fight against organised crime and money laundering.

1 D. Van Daele et al., *Criminaliteit en rechtshandhaving in de Euregio Maas-Rijn, Deel 3: De bestuurlijke aanpak van georganiseerde criminaliteit in Nederland en België*, 2010.
2 Cf. also M. Vols and L.M. Bruijn, "De strijd van de burgemeester tegen drugscriminaliteit", *Netherlands Administrative Law Library* (2015), 1–23.
3 More information about the EURIEC project, including the possibilities and "bottlenecks" with regard to an international administrative approach, can be found on the EURIEC website: www.euriec.eu.
4 Yet, data on companies in general does not fall under the conditions of the GDPR and therefore does not necessarily need a legal basis in order for this information to be exchanged across borders. In most cases, however, personal data will be more useful for local authorities, but such an exchange seems highly difficult with the existing regulations and legislation in Belgium, North Rhine-Westphalia, and the Netherlands.
5 *O.J.* L 76, 22.3.2005, 16.
6 I.e. the transmitting authority needs to give its consent and the consent must be in accordance with the national law of the transmitting and receiving Member States.

Le notariat italien et européen en première ligne dans la lutte contre le blanchiment d'argent

Valentina Rubertelli

This article describes the role and activities of the Italian notary in the fight against money laundering. The Italian notaryship has always been committed to this fight: compared to other professional groups obliged by the relevant anti-money laundering legislation, notaries submit 91% of the reports on suspicious transactions; it recently also proposed the creation of an anti-money laundering data warehouse based on the Spanish model and considered to be an excellent tool by the Financial Action Task Force (FATF). In addition, the Italian notary will closely follow the process of new EU regulations on anti-money laundering during its presidency of the Council of the Notariats of the European Union (CNUE) in 2022. It will work to ensure that the new legislation takes into account the specificities of the notarial profession with its public function.

I. Le rôle du Notariat italien dans le contrôle du blanchiment d'argent.

Le Consiglio Nazionale del Notariato (CNN, ordre national des notaires italiens) suit et analyse de manière constante la règlementation sur la lutte contre le blanchiment et le financement du terrorisme. Pour cela il collabore de manière active, et cela depuis toujours, avec les sujets institutionnels chargés de la préparation et de l'application de la règlementation en Italie, tels que le Ministère de l'Economie et des Finances, l'unité d'information financière (UIF – Unità di Informazione Finanziaria) de la Banque d'Italie et la brigade financière (Guardia di Finanza).

En Italie, le Notariat a été en 2009 le premier ordre professionnel à assumer le rôle et la responsabilité d'autorité de contrôle en matière de lutte contre le blanchiment. En 2014, le CNN a élaboré dans ce domaine les lignes directrices et les règles techniques à suivre pour remplir les conditions nécessaires à la lutte contre le blanchiment. Il a créé un réseau de notaires qui est distribué de manière étendue sur tout le territoire et chargé des activités de lutte contre le blanchiment et de la diffusion de la « culture » anti-blanchiment auprès de tous les confrères italiens.

Parmi les professionnels qui ont l'obligation d'accomplir les contrôles anti-blanchiment, les notaires sont ceux qui signalent

d'avantage les déclarations d'opérations suspectes (les SOS – Segnalazioni Operazioni Sospette), comme cela a été reporté dans la Newsletter UIF 70.157 déclarations d'opérations suspectes ont été effectués à l'UIF par les notaires dans le cadre du premier semestre de 2021. En ce qui concerne le secteur non financier, on observe que parmi les augmentations les plus significatives figures de nouveau les activités du Notariat dont les déclarations d'opérations suspectes sont passées de 1.561 au premier semestre de 2020 à 2.479 pour la même période en 2021. Sur un total de 2.711 SOS envoyées par les différentes catégories professionnelles durant la période indiquée, les déclarations (SOS) effectuées par les notaires représentent donc 91,4 % du total des déclarations envoyées par l'ensemble des professionnels.[1]

Le modèle de contrôles préventifs italien a, par ailleurs, été mis en avant par le GAFI, la Banque Mondiale et OCDE.[2] De plus et ce pour la première fois en 2019, le Notariat italien a officiellement été inclus parmi les institutions pivots pour la lutte contre la corruption et contre le blanchiment dans le rapport de l'Office des Nations Unies contre la Drogue et le Crime (ONUDC).

Sur la base d'une estimation de l'UIF, dans le cadre des déclarations provenant du Notariat italien, les cas qui reviennent le plus souvent concernent la stipulation d'actes dans le secteur immobilier et des sociétés. La plupart des opérations immobilières signalées concernent des transactions caractérisées par l'implication de contreparties avec des références judiciaires préjudiciables ou situées dans des pays ayant une fiscalité privilégiée. Les anomalies relevées sont généralement liées à l'origine suspecte des fonds utilisés et à des modalités atypiques de paiement ou bien à la détermination de la somme correspondante. Dans le domaine des sociétés, outre la provenance des apports, des suspicions liées aux modalités d'acquisition ou de cession des sociétés, l'utilisation de prête-noms et l'introduction dans les entreprises de sujets impliqués dans des enquêtes, sont fréquemment déclarées.

II. Les instruments du Notariat italien contre le blanchiment

Comment est-il possible que le Notariat soit devenu un point de référence parmi les institutions tenues à la lutte contre le blanchiment en n'étant pas de nature bancaire ou financière ?

En premier lieu, le fait que le notaire, contrairement à d'autres professionnels, soit obligé de par sa fonction, à examiner l'opération d'un point de vue position impartiale par rapport aux parties, lui permet de vérifier si quelque chose dans le mécanisme contractuel ne présente pas une anomalie et le cas échéant de refuser sa prestation. Lorsque le législateur a impliqué les professionnels dans les activités de contrôle en matière de lutte contre le blanchiment, le notaire a simplement étendu son champ d'observation à ces phénomènes sans dénaturer sa fonction. Ce contrôle fait par les notaires sert à garantir que soit émis dans le circuit juridique uniquement ce qui est légal. C'est pour cela que l'on qualifie le notaire comme étant un « gatekeeper ». La valeur ajoutée des procédés anti-blanchiment mis en œuvre par le Notariat résulte sans aucun doute d'une part de la nature d'autorité publique de l'activité du notaire, soumis à la surveillance et au contrôle continu et direct de l'Etat à travers le Ministère de la Justice et, d'autre part de sa position – selon la loi – super partes par rapport aux parties du contrat et par une évaluation détachée des profils d'anomalie aux fins d'une éventuelle déclaration de l'opération comme étant suspecte.

En second lieu, en adoptant des lignes directrices internes et en consolidant de manière concrète le système de transmission des SOS dans l'anonymat par l'intermédiaire du Consiglio Nazionale del Notariato, le Notariat italien est parvenu à une formation et une sensibilisation complète et répandue au bénéfice de la catégorie professionnelle et de tous les collaborateurs des offices notariaux.

A présent, le Consiglio Nazionale del Notariato dispose d'un instrument pour engager un processus ultérieur qui puisse être considéré comme un saut de qualité quant à la participation du notariat à la lutte contre le blanchiment et contre les délits fiscaux.

En partant de l'expérience développée par le notariat espagnol, et en y conjuguant la particularité du notariat italien, qui, unique en Europe, dispose d'un intranet qui relie en toute sécurité tous les offices notariaux et recueille tous les mois les données des actes notariés à des fins statistiques, le CNN, en exécution des articles 15 et 16 du Décret-législatif n. 231/07, se propose d'adopter une méthodologie informatique nouvelle et innovante d'analyse et d'évaluation du risque. Il se propose ainsi de constituer une Datawarehouse du Notariat : une archive informatique dans laquelle peuvent confluer toutes les données liées aux actes notariés italiens afin qu'un système d'Intelligence Artificielle puisse les traiter. Cela permettrait ainsi à chaque notaire de pouvoir repérer des éléments d'anomalies et de suspicion qui pourraient échapper à une analyse individuelle de chaque opération décontextualisée des autres.

En plus de la Datawarehouse et, en utilisant le remarquable bagage d'expérience qu'il a accumulé au cours des années, le notariat italien suggère par ailleurs, que l'obligation de tracement des modalités de paiement de la somme correspondan-

te (avec l'indication dans l'acte des éléments essentiels des chèques et des virements bancaires) soit également étendue à d'autres types d'actes que celle des ventes immobilières : on pourrait l'envisager pour les cessions des entreprises et également pour les cessions des apports de participation dans les sociétés.

Au cours de la Conférence des Parties de la « Convention des Nations Unies contre la criminalité organisée transnationale » du 16 octobre 2020 à Vienne, et à l'occasion de l'approbation du document présenté par l'Italie et qui passera à l'histoire comme la « Résolution Falcone »,[3] il a également été affirmé avec vigueur le principe selon lequel la manière la plus efficace pour lutter contre la criminalité organisée est, comme l'a toujours soutenu le juge italien engagé dans la lutte antimafia et assassiné Giovanni Falcone, celle résumée dans la devise « Follow the money ».

III. La contribution du notariat italien à la réforme legislative

C'est justement parce que le notariat italien joue un rôle principal dans la lutte contre le blanchiment qu'il participe de manière constante aux travaux du Conseil des Notariats de l'Union Européenne (CNUE)[4] visant à suivre toutes les initiatives législatives au niveau européen et, en particulier, les récentes propositions du paquet législatif en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (publié par la Commission européenne le 20 juillet 2021).[5]

A l'instar de ce que propose la Commission, le notariat italien, qui a la présidence du CNUE pendant l'année 2022, est d'avis que l'Autorité de lutte contre le blanchiment (ALCB) ne devrait exercer une surveillance que sur certaines entités assujetties au secteur financier et limiter ses activités à une fonction de coordination par rapport aux entités assujetties au secteur non financier. En effet, une différenciation claire et nette doit être faite entre le secteur financier et le secteur non financier. A la différence du secteur financier, le secteur non-financier est hétérogène (ou sui generis) et connaît des spécificités (ou aspects particuliers) qu'il est important de respecter et maintenir car elles participent à l'efficacité du système au niveau national.

De plus, en ce qui concerne les notaires, un régime de surveillance strict et performant (notamment concernant la lutte contre le blanchiment d'argent et le financement du terrorisme) est déjà assuré au niveau national par les ministères de la justice, les tribunaux et/ou les organismes d'autorégulation professionnelle ainsi que les Cellule de Renseignements Financier (CRFs). Cette surveillance tient par ailleurs compte des spécificités de la fonction de notaire en tant qu'officier public nommé par l'Etat et donc, dans une certaine mesure, considéré comme une extension de l'État. Les notaires sont également, chargés, dans certains États membres, des fonctions judiciaires et font donc partie du pouvoir judiciaire, dont l'indépendance est une caractéristique de l'Etat de droit et est garantie par la Constitution.

Du point de vue du notariat, un futur règlement anti-blanchiment devrait permettre aux États membres de l'UE d'aller encore plus loin que les dispositions minimales du règlement[6] en matière de mise en œuvre du contrôle par le notaire afin d'élaborer des solutions adaptées et efficaces, en tenant compte notamment des différents systèmes notariaux. Le législateur de l'Union devrait donc veiller à ne pas priver les États membres de la possibilité de répondre de manière adéquate aux particularités nationales en introduisant un cadre juridique pleinement harmonisé.

Me. Valentina Rubertelli
Présidente du Consiglio Nazionale del Notariato

1 Voir à ce propos <https://uif.bancaditalia.it/pubblicazioni/quaderni/2021/quaderno-1-2021/index.html>.
2 E. van der Does de Willebois et al., *The Puppet Masters : how the corrupt use legal structures to hide stolen assets and what to do about it*, Washington DC World Bank 2011.
3 Resolution 10/4 "Celebrating the twentieth anniversary of the adoption of the United Nations Convention against Transnational Organized Crime and promoting its effective implementation", <https://www.unodc.org/documents/treaties/UNTOC/COP/SESSION_10/Resolutions/Resolution_10_4_-_English.pdf>.
4 Le CNUE est l'organisme officiel et représentatif de la fonction notariale auprès des institutions européennes. Il représente 22 chambres nationales de notaires et compte plus de 45 000 notaires.
5 Voir eucrim 3/2021, 153 et suiv.
6 Proposal of the European Commission 2021/0239 (COD) of 20 July 2021 "Regulation on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing".

The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention

A Flawed Comparison?

Lukas Martin Landerer

Early in its development, the EU's anti-money laundering (AML) scheme was already criticized for its interference with the fundamental rights to privacy. Quite recently, some scholars have highlighted that customer due diligence obligations constitute a massive retention of financial data. Consequently, they have tried to apply the ECJ's findings on data retention of telecommunication traffic data to the AML framework. Financial data is quite legitimately seen as a honeypot for law enforcement authorities, which makes a comparison between retention of financial data and retention of telecommunication traffic data readily apparent. Surprisingly, not much attention is paid to the AML framework in this context, compared to the pile of comments on the retention of telecommunication traffic data. Not even the EDPS mentioned data retention as a problem in his opinion of the EU's action plan on money laundering in 2020. It is thus also not surprising that no alterations to the retention obligations can be found in the recently proposed AML Regulation. The question arises: does the AML scheme really compare as easily to the prominent data retention of telecommunication meta data after all? As yet another AML package lies ahead of us, it is time to have a look at why the EU legislator does not seem to be intimated by the ECJ's case law regarding its AML framework. The author argues that the definition of data retention, which the scholars who wish to apply the ECJ's case law to the AML framework have in mind, is too broad. It does not capture why the ECJ has so strictly ruled on the retention of telecommunication traffic data. The AML scheme deviates from the retention of telecommunication traffic data in several ways. These differences make it difficult to test the lawfulness of the Union's AML law in its new guise by applying the ECJ's jurisprudence on data retention. In light of the ECJ's case law, it is the access permissions whose legitimacy seems questionable, not the obligation clauses.

I. Introduction

The term *data retention* can generally be defined as "the collection and storage of personal data for an undetermined purpose in the event that it should ever be needed for not yet specified future use."[1] Its notoriety stems from a – more than decade-long – legal dispute between EU Member States and the European Court of Justice (ECJ). The story really began in 2006, when the EU obligated its Member States to set up or align laws on retention of telecommunication traffic data via a directive.[2] Providers of electronic communication, including internet access and internet telephony, were thereby forced to retain traffic data (who called who, when, and from where?) of their customers for six months and to make them accessible to state security authorities.

As is known, the ECJ was not happy with this directive. In the *Digital Rights Ireland* judgment of 2014, the Court found that the massive retention of data without specific cause would constitute a disproportionate interference with the rights of private life and data privacy, Arts. 7 and 8 of the Charter of Fundamental Rights of the EU, and thus revoked the directive.[3] Subsequently, some Member States argued that the judgment would not affect respective norms in domestic law and kept their retention obligations.[4] Inevitably, the ECJ had to decide on these national data retention laws as well. It took the opportunity to affirm its case law, in principle, but specified it in two consecutive judgements, *Tele2 Sverige5* and *La Quadrature du Net.6*

The findings of the Court regarding the conditions for data retention can be briefly summarized as follows:[7] Principally, data retention must be viewed as a two-stage process. First, there is a legal obligation, mainly for private actors, to store a bulk of data for a specific period of time. The second stage comprises the legal provisions that enable state authorities to access these data. Both elements independently interfere with fundamental rights to privacy.[8] Therefore, there must be safeguards for each stage.[9] As of now, a general retention of data is only permissible if a Member State is threatened by a real and present danger to national security.[10] If this is not the case, only data from specific persons may be retained, based on objective, non-discriminating, or geographical criteria.[11] In any case, state access to these data may only be permissible if it

is necessary to combat serious crime, if it is subject to prior review by a court or an independent administrative authority, and if the retained data is based within the EU.[12]

In the following section, I will briefly describe, where data retention rules are included in the European AML framework (II). It shall then be shown that retention of transaction data is nothing new as it has been included in various legal provisions already (III). Hence, I will argue that maybe instead one should shift away from focussing on retention clauses and rather critically review the clauses, which grant the FIUs access to retained transaction data (IV).

II. Data Retention in the New AML Regulation

The European Union's anti-money laundering (AML) framework obliges entities to retain personal financial data. As of now, the central norm can be found in Art. 40 of the anti-money laundering Directive,[13] which was amended for the fifth time in 2018 (AMLD5).[14] Art. 40(1)(a) AMLD5 obliges entities to retain a copy of

> "the documents and information which are necessary to comply with the customer due diligence requirements (…) for a period of five years after the end of their business relationship (…) or after the date of an occasional transaction."

Furthermore, Art. 40(1)(b) AMLD5 obliges entities to keep records

> "of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction."

The recent proposal for an AML regulation (hereinafter: AMLR-p)[15] does not make substantial changes to these obligations. Art. 56(1) AMLR-p reads almost identically with Art. 40(1) AMLD5. Just like its predecessor, it differentiates between information that was necessary for the execution of customer due diligence (CDD) measures in para. 1(a) and transaction records in para. 1(b). The declaration of para. 1(b) is unambiguous. It provides an obligation to retain records of any transaction, independently from the scope of the applied CDD measures.

This issue has been acknowledged not only by legal scholars[16] but also by Article 29 (Data Protection) Working Party as early as 2011.[17] Although the Working Party did not directly compare the AML framework to the data retention rules regarding telecommunication meta data, it was deeply concerned by the long and rigid retention periods.[18] The Union legislator has yet to react to this criticism. The retention periods have not been altered since 2011 and still amount to five years according to Art. 56(3) AMLR-p.

The fact that the retention rules have not changed substantially might be explained by the low public awareness of the topic, both in academic and in political discussions. Although data retention, especially that of telecommunication data and of passenger flight records, is heavily discussed in Germany,[19] the AML framework is noted merely as a side issue.[20] The European literature looks somewhat better, with about a handful of authors commenting on the issue.[21] Yet, the amount of literature regarding the topic falls significantly short to the prominence of data retention concerning telecommunication data.

III. Retention of Transaction Data in other Legal Provisions

The reason for this lack of attention is surely not to be found in the characteristics of the retained data. As all the scholars involved in researching this topic[22] have noticed, financial data are as sensitive as it can get according to the standards of the ECJ. The judges in Luxembourg rightfully considers the quality of personal data and therefore the intensity of its retention according to the way the data can be used to develop personality profiles.[23] There are few documents imaginable that are as suitable for creating such personality profiles as transaction records. They contain information on personal preferences, income, location, personal relations, and much more. Especially in a consumer age of cashless payments, bank account statements can be read as a summary of one's personal life.[24] Thus, unsurprisingly, security and intelligence agencies are quite keen on obtaining financial records.[25] The general German acceptance of the disclosure of financial data relates to this trend coherently. In an empirical study, however, 66% of the respondents answered that the duty of banks to hand out information to state authorities is "not a good thing".[26]

A better explanation for the absence of the topic in legal discussions might be the universality of retention obligations regarding financial data in various legal provisions. Other than telecommunication traffic data, transaction records are not stored for security purposes only. This will be exemplified in the following by taking a look at German and European Union law.

1. Germany

According to German law, banks and other financial services that provide accounts for their customers have a civil law accountability to report the balances to their customers in detail. This duty stems directly from the banking contract itself, e.g. giro accounts, in accordance with §§ 666, 675 of the German Civil Code (*Bürgerliches Gesetzbuch – BGB*).[27] Financial companies usually fulfil this duty by providing account statements.[28]

Furthermore, banks and payment services are merchants according to § 1 paras. 1, 2 of the German Commercial Code (*Handelsgesetzbuch – HGB*). As such, they are required to adhere to commercial accounting rules (§ 238 para. 1 HGB). These include an obligation to retain *accounting receipts* for ten years (§ 257 para. 1 (4) HGB). Such receipts include all documents referencing business events and transactions.[29] Now, every transaction and deposit that is carried out via a banking or payment account is considered a business event from the bank's point of view, since they directly affect the contractual relationship with their customer. Thus, the account statement, where all accounting events are listed, fall under the scope of application of § 257 para. 1 (4) HGB.[30] To handle this vast amount of data, banks have made a transition to storing their customers' statements digitally.[31]

Overlapping with the trade law's obligation is the accounting obligation in German tax law. § 147 para. 1 (4) of the Fiscal Code (*Abgabenordnung – AO*). It reads similar to § 257 HGB regarding accounting receipts and contains the same retention period. The rules are coordinated.[32] The German banking law also contains an accountability clause in § 25a para. 1 sentence 6 (2) of the Banking Act (*Gesetz über das Kreditwesen – KWG*).

2. European Union

At the EU level, various provisions regulate which specific information must be contained in account statements. Arts. 57, 58 of the second Payment Services Directive (PSD2)[33] regulate information that must be provided by the payment service providers to both payer and payee. This involves transactions conducted via giro accounts.[34] The banks of both payer and payee which act as payment service providers,in turn fulfil their respective duties by providing account statements.[35] Art. 21 PSD2 includes a five-year record-keeping clause, affecting *all appropriate records for the purpose* of title 3 of the PSD2, but it does not affect domestic retention clauses, since it only sets a minimum retention period. It also explicitly does not affect the retention rules of the AML framework.

Another source of information provisions on payments can be found in the Regulation Regarding Direct Debit and other Transfers in Euro (SEPA-Regulation).[36] Art. 5 (1) and (3) SEPA-Regulation in conjunction with No. 1, 2 of its Annex provide some obligatory information that the acting payment providers must submit to payer and payee. The information mostly overlaps with what is already mandatory according to PSD2. The same can be said for the Transfer of Funds Regulation,[37] which also includes a five-year retention clause in Art. 16.

In sum, German law in conjunction with EU law poses a whole package of retention rules regarding account statements.

IV. A New Focus: The FIU's Access to Retained Financial Data

The fact, that banks and other payment service providers store transaction record and thus retain sensitive financial data is thus, nothing new. The AML-framework does not constitute an obligation, which wouldn't otherwise exist. Its effect is of mere declarative or repetitive nature.

Yet, the focus of attention has primarily been on monitoring and retention clauses which cannot come as a surprise. From the very beginning, the ECJ has highlighted that not only state access, but also retention (by private actors) itself affects fundamental rights.[38] It is questionable whether this approach is persuasive in its generality , if one takes into account that companies' accounting and compliance rules as well as social and public administration law, in many cases, inevitably lead to the processing and storage of large amounts of personal data. Also, accessing this data is usually not a problem for security authorities – at least not in Germany. Although the correct legal rules for information requests may be debated in criminal procedure[39] and police law,[40] their general permissibility is not disputed. For intelligence services, there are even explicit norms that allow for secret information requests from banks, e.g., § 8a para. 1 (2) of the Federal Office for the Protection of the Constitution Act (*BVerfSchG*).

1. The root of the issue with data retention structures

One can thus conclude that the general idea of data retention for private entities or public administration authorities cannot be the reason for the ECJ's disfavour. It is in the nature of today's society that information is documented for various reasons. And it belongs to the very nature of criminal investigation that pre-existing information is gathered. Hence, the broad definition that was presented in the introduction must be narrowed down, if one wishes to get to the core of what makes the famous data retention cases so significant.

One factor that must be highlighted is the purpose of the retention clause.[41] Only if strictly for security issues should the narrow conditions of the ECJ be applied. This is obviously the case for the AML data retention clauses, as they are aimed at fighting money laundering and the financing of terrorism. Yet, they constitute a special case, since the obligation to retain transaction records overlaps with legal rules that have different purposes, for example economical ones. Thus, the question is whether the mere addition of a security purpose to an already existing retention obligation should be viewed as strictly as retention clauses that exist only for security reasons, as was the case with the 2006 Data Retention Directive.

To answer this question, one must shift the focus away from the retention level and look towards access structure. In Germany, the purpose of access rules on telecommunication meta data can be twofold.

First and in any case, they allow for secret access. Traffic data could previously be accessed directly from telecommunication providers according to § 113 of the 2015 Telecommunications Act (*Telekommunikationsgesetz – TKG 2015* [not in force anymore]). The providers were legally forced to treat the request confidentially according to §§ 15, 33 Telecommunications Interception Ordinance. Such an obligation to secrecy does not exist if the request were to be based on the general provisions of the criminal procedure code.[42]

The second purpose, which can be found in the access provisions for contractual data, is simplification. The access privilege for telecommunication contract data (name, number, identification code, device number, etc.) lies with a central authority, the Bundesnetzagentur (*Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway*), which has direct access to the providers' databases, § 173 TKG. The same holds true for contractual data of bank account holders, § 24c KWG, §§ 93b, 93 paras. 7, 8 AO.[43] In these "automated processes", security authorities do not themselves address the (private) providers but must rather ask the respective central authorities to do so. The investigating officer can instead stay in his/her office without having to disclose the investigation to anyone. This ability to investigate via communication alone makes the citizen easily transparent. Especially if the investigation solely takes place between authorities. Perhaps it was this image that led the ECJ to conduct its strict review on retention of telecommunication data, as it deviates from the conventional image of investigation under the rule of law. Traditionally, the state must face the concerned person to ensure equality of arms.[44] This includes the principle of an openly investigating police.[45]

2. The FIU's access provisions

Here lies the problem with data retention structures. The more they deviate from our traditional picture of legal investigation, the more they infringe the right to privacy. It has already been recognized that the retention obligation in the AML framework only adds a purpose and does not lead to more factual records. In this context, it is less infringing than the retention of telecommunication traffic data. If one wishes to apply the ECJ's jurisdiction in *La quadrature du net* to the AML framework, one must then check whether the access rules of the AML framework deviate from traditional principles of investigation in such a way that it lends itself to a comparison with the retention of telecommunication traffic data.

In principle, the AML framework is a compliance system. The private entities – not security authorities – are at the forefront of the fight. Unlike telecommunication providers, banks must actively monitor transactions and report suspicious activities. These "suspicious activity reports" (SARs) can even be seen as the core of the system.[46] Meanwhile, the ECJ[47] and the ECtHR[48] have found that the obligation to submit SARs would, at least, not even infringe the rights of obliged lawyers. The privacy rights of the affected customers were not substantially checked; thus, it seems that the case law does not recognize them as a problem with regard to SARs.

However, the AML framework does allow for the reverse direction as well. According to Art. 32(9) AMLD5, the Financial Intelligence Units (FIUs) are "able to request, obtain and use information from any obliged entity for the purpose set in paragraph 1 of this Article, even if no prior report is filed". This authorisation of FIU's to request information is included Art. 18 (4) of the proposal for a sixth AML-directive – AMLD6-p[49] and reads identically to its predecessor. A similar provision can be found in Art. 33 (1) (b) AMLD4 respectively Art. 50(1)(b) AMLR-p, which reads:

> Obliged entities, and, where applicable, their directors and employees, shall cooperate fully by promptly providing the FIU directly, at its request, with all necessary information.

Although the wording suggests that Art. 33 (1) (b) AMLD4 respectively Art. 50(1)(b) AMLR-p are no authorisation rules. In any case, the FIUs are authorised by 32(9) AMLD5 respectively Art. 18 (4) AMLD6-p. These provisions state that a prior report is not needed for the FIUs' requests which is also clarified by recital 79 AMLR-p. The FIUs' competence to request information must be read in conjunction with the other competent security authorities' permission to request information from the FIU. This authorisation is stated in Art. 32(4) AMLD4/5 and can be found, almost unchanged, in Art. 19(1) AMLD6-p.

In theory, without a SAR having been filed, security authorities can access the financial information of a target indivudal by requesting this information from the FIU. The FIU could then send a request to the respective private entities. Via this route, security authorities could access the retained account statements without themselves having disclosed the investigation towards the obliged entities.

The private entities are not allowed to disclose the FIU's request to third parties, especially not to their customers (Art. 39 (1) AMLD5/Art. 54(1) AMLR-p). Therefore, the access remains secret. This access route should be focused on in any proportionality test of potential fundamental rights infringements.[50] As long as the access is not subject to the

conditions that were demanded in the ECJ's case law on data retention, the argument can well be made that the current and proposed AML framework violates privacy rights.

V. Conclusion

It has been shown that applying the ECJ's pattern regarding retention of (teleocommunication) data to the AML framework is intrusive, but not as easy as some scholars[51] have suggested. The obligation to retain financial data does not factually increase the amount of stored data, since overlapping obligations are already in place. The purpose has merely been expanded to now include security-related issues.

One should thus shift from focusing on the retention obligation as such and instead review the FIUs' access to the records more strictly. Via information requests, other competent state authorities could indirectly access financial data, without a suspicious activity reports being filed (by a private entity). This leads to secret access to privately stored data through an intermediary authority. Since this structure deviates from the traditional approach to law enforcement, a case can be made for applying the ECJ's data retention conditions, at least as regards the accessibility of data pursuant to the AML legal framework. The fact that corresponding considerations are missing in the recently proposed AML package raises doubts as to whether or not the Union legislator is really willing to implement the ECJ's findings.

Lukas Martin Landerer LL.M.
Doctoral Researcher, Max Planck Institute for the Study of Crime, Security and Law, Department of Public Law, Freiburg i.Br.

1 M. Albers, "Data Retention in Germany", in: M. Zubik, J. Podkowik and R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws,* 2021, p. 117.
2 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.
3 ECJ, 8 April 2014, cases C-293/12 and C-594/12, *Digital Rights Ireland, paras. 45–69.*
4 For an overview, see J. Kühling and S. Heitzer, "Returning Through the National Back Door? The Future of Data Retention After the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere", (2015) 40(2) *European Law Review,* 263; X. Tracol, "Legislative Genesis and Judicial Death of a Directive", (2014) 30(6) *Computer Law & Security Review,* 736, 743–744.
5 ECJ, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige, Tom Watson and Others.*
6 ECJ, 8 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others.*
7 For an overview, see T. Wahl, "Spotlight: CJEU: Data Retention Allowed in Exceptional Cases", (2020) *eucrim*, 184.
8 ECJ, *Digital Rights Ireland, op. cit.* (n. 3) paras. 58–60; MP. Granger and K. Irion, "The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection", (2014) 39(6) *European Law Review*, 834.
9 See AM. Pedersen, H. Udsen and SS. Jakobsen, "Data retention in Europe – the Tele 2 case and beyond", (2018) 8(2) *International Data Privacy Law,* 160.
10 ECJ, *La Quadrature du Net and Others, op. cit.* (n. 6), paras. 137, 168.
11 ECJ, *La Quadrature du Net and Others, op. cit.* (n. 6), para. 168.
12 ECJ, *Tele2 Sverige, op. cit.* (n. 5), para. 125.
13 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *O.J. L* 141, 5.6.2015, 73.
14 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, *O.J. L* 156, 19.6.2018, 43.
15 Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 20.7.2021, COM(2021) 420 final. For a summary, see T. Wahl, "Spotlight: AML Package II: Commission Proposes AML Regulation", (2021) *eucrim*, 154–155.
16 C. Kaiser, *Privacy and identity issues in financial transactions,* 2018, pp. 101–104, 492–495; J. Milaj and C. Kaiser, "Retention of data in the new Anti-money Laundering Directive – 'need to know' versus 'nice to know'", (2017) 7(2) *International Data Privacy Law,* 115, 123.
17 Article 29 Data Protection Working Party, "Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing", (01008/2011/EN WP 186 13 June 2011), Annex No. 28, 29, pp. 22–24.
18 Article 29 Data Protection Working Party, *op. cit.* (n. 17), No. 28, 29, pp. 22–24.
19 See *inter alia* A. Moser-Knierim, *Vorratsdatenspeicherung,* 2014.
20 See, for example, Albers, *op. cit.* (n. 1), p. 117.
21 A. Bertrand, W. Maxwell and X. Vamparys, "Do AI-based anti-money laundering (AML) systems violate European fundamental rights?", (2021) 11(3) *International Data Privacy Law,* 276; B. Vogel, "Conclusions and Recommendations", in: B. Vogel and J.-B. Maillart (eds.), *National and international anti-money laundering law. Rethinking the architecture of criminal justice, regulation and data protection,* 2020, pp. 881, 897–904; Kaiser, *op. cit.* (n. 16); J. Milaj and C. Kaiser, (2017) 7(2) *Int. Data Privacy Law, op. cit.* (n. 16).
22 Ibid.
23 ECJ, *La Quadrature du Net and Others, op. cit.* (n. 6), para. 117; *ECJ, Digital Rights Ireland,* op. cit. (n. 3) para. 27; see M.W. Müller and T. Schwabenbauer, "Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden", (2021) *Neue Juristische Wochenschrift* (*NJW*), 2079, 2084.
24 V. Pfisterer, "'Finanzprivatsphäre' in Deutschland", (2017) 65(1) *Jahrbuch des öffentlichen Rechts der Gegenwart. Neue Folge* (*JöR*), 393, 400; C. Westermeier, "Money Is Data – the Platformization of Financial

Transactions", (2020) 23(14) *Information, Communication & Society*, 2047; Wissenschaftliche Dienste des Bundestags, "Zu möglichen erweiterten Befugnissen der Nachrichtendienste bei der Überwachung von „Finanzströmen", (WD 3 – 3000 – 040/19 2019), 7.3.2019, p. 11.

25 See T. Reichling, "Strafprozessuale Ermittlungen bei Kreditinstituten – ein Überblick", (2011) *Juristische Rundschau* (JR), 12; M. Parker and M. Taylor, "Financial Intelligence: A Price Worth Paying?", (2010) 33(11) *Studies in Conflict & Terrorism,* 949, 952–954; B. Scott and M. McGoldrick, "Financial intelligence and financial investigation: opportunities and challenges", (2018) 13(3) *Journal of Policing, Intelligence and Counter Terrorism*, 301.

26 M. Heiden, *Banken als Erfüllungsgehilfen staatlicher Politik,* 2013, p. 100.

27 Bundesgerichtshof (BGH) [German Federal Court of Justice], (2003) *Neue Juristische Wochenschrift – Rechtsreport (NJW-RR), 1555, 1556;* G. Bitter, Kontenpfändung, in: H. Schimansky, H.-J. Bunte and H.-J. Lwowski (eds.), *Bankrechts-Handbuch,* 5th ed. 2017, § 33, mn. 56.

28 Bundesgerichtshof (BGH) [German Federal Court of Justice], (2001) *Neue Juristische Wochenschrift – (NJW), 1486;* M. Löhnig, "BGH v. 8.11.2005 – ZR 90/05, Anspruch auf Erteilung von Kontoauszügen wird nicht mit Hauptforderung mitgepfändet", (2007) *Juristische Rundschau* (*JR*), 73, 75.

29 B. Rätke, in: E.-M. Gersch and others (eds.), *Abgabenordnung: Einschließlich Steuerstrafrecht,* 15th ed. 2020, § 147, mn. 24.

30 See T. Knierim, in: B. Bannenberg and others (eds.),Straftaten im Bankbereich, *Handbuch des Wirtschafts- und Steuerstrafrechts,* 5th ed., 2020, Chapter 10, mn. 25.

31 Ibid.

32 S. Shin, *Bank- und kapitalmarktrechtliche Organisationspflichten,* 2013, p. 169; Rätke, *op. cit.* (n. 29), § 147, mn. 147.

33 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, *O.J. L 337, 23.12.2015, 35.*

34 K. Wahlers, *Die rechtliche und ökonomische Struktur von Zahlungssystemen inner- und außerhalb des Bankensystems,* 2013, p. 30.

35 Bundesgerichtshof (BGH) [German Federal Court of Justice], (2014) *Neue Juristische Wochenschrift (NJW), 922.*

36 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009, *O.J. L* 94, 30.3.2012, 22.

37 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, *O.J. L* 141, 5.6.2015, 1.

38 ECJ, *Digital Rights Ireland, op. cit.* (n. 3), paras. 58–60.

39 T. Reichling (2011) *JR, op. cit.* (n. 25); T. Kahler, *Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten,* 2017, pp. 31–55.

40 J. Wonka, "Die Rechtmäßigkeit staatlicher Auskunftsersuchen gegenüber Banken", (2017) *Neue Juristische Wochenschrift* (*NJW*), 3334, 3337–3338.

41 See *Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court], (2010) Neue Juristische Wochenschrift (NJW),* 833, mn. 227; W. Bär in: J. Graf (ed.), *BeckOK StPO mit RiStBV und MiStra,* Ed. 1.10.2020, § 100g StPO, mn. 1.

42 See T. Reichling, (2011) *JR, op. cit.* (n 25), 16.

43 See *Bundesverfassungsgericht (BVerfG) [Federal Constitutional Court], (2007) Neue Juristische Wochenschrift (NJW)*, 2464; A. Kokemoor, "Der Automatisierte Abruf von Kontoinformationen nach § 24c KWG", (2004) *Zeitschrift für Bank- und Kapitalmarktrecht* (*BKR*), 135; V. Pfisterer, (2017) 65(1) *JöR, op. cit.* (n. 24), 407–412.

44 *Bundesgerichtshof (BGH) [Federal Court of Justice], (2010) Neue Juristische Wochenschrift (NJW), 1297, 1298;* K. Gaede, *Fairness als Teilhabe,* 2010, pp. 305–310.

45 S. Stavros, *The Guarantees for Accused Persons Under Article 6 of the European Convention on Human Rights,* 1993, p. 75; M. Fincke, "Zum Begriff des Beschuldigten und den Verdachtsgraden", (1983) 95(4) *Zeitschrift für die gesamte Strafrechtswissenschaft* (ZStW), 918, 955–972; Gaede, *op. cit.* (n. 44), pp. 233–238.

46 S. Barreto da Rosa, in: F. Herzog and O.C. Achtelik (eds.), *Geldwäschegesetz (GwG),* 4th ed., 2020, § 43, mn.1.

47 ECJ, 26 June 2007, Case C-305/05, *Ordre des barreaux francophones et Germanophone v Conseil des ministers.*

48 ECtHR, 6 December 2012, *Michaud v France, Appl. No. 12323/11.*

49 Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, 20.7.2021, COM(2021) 423 final.

50 See also B. Vogel, "The Anti-Money Laundering Architecture of Germany", in: B. Vogel and J.-B. Maillart (eds.), *op. cit.* (n. 21) , pp. 157, 242–246; Barreto da Rosa, *op. cit.* (n. 46), § 30, mn. 21.

51 Kaiser, *op. cit.* (n. 16); Milaj and Kaiser, (2017) 7(2) *Int. Data Privacy Law, op. cit.* (n. 16); A. Bertrand, W. Maxwell and X. Vamparys, (2021) 11(3) *Int. Data Privacy Law, op. cit.* (n. 21).

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; Dr. Lothar Kuhl, Head of Unit, DG REGIO, European Commission, Belgium; 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