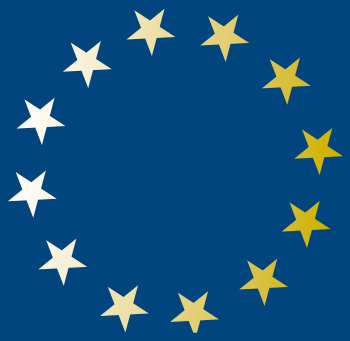
eucrim 2023 / 1
European Law Forum: Prevention • Investigation • Prosecution



Artificial Intelligence
Intelligence artificielle
Künstliche Intelligenz

2023 / 1 ISSUE / ÉDITION / AUSGABE

eucrim also serves as a platform for the Associations for European Criminal Law and the Protection of Financial Interests of the EU – 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. More information about the Associations is available at: https://eucrim.eu/associations/.

Contents

News*

European Union

Council of Europe

Articles

Artificial Intelligence

Beyond the Focus

* The news items contain Internet links referring to more detailed information. 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,


Sabine Gless


Katalin Ligeti

Artificial Intelligence (AI) has the potential to help us in many ways. One of the promising fields in which AI can be employed is in the fight against crime, as is spotlighted by a number of contributions in this issue, e.g. on AI's impact on anti-money-laundering regimes or on the employment of AI to prevent cross-border human trafficking. AI also shows its immense potential when applied in the field of forensic analysis, where robots equipped with advanced imaging and analysis capabilities can assist. They are not only capable of processing evidence, collecting fingerprints, analysing DNA samples, and performing other tasks that require technical precision and complex calculations; they also open up effective options for surveillance: Robots equipped with cameras and sensors can be deployed for surveillance purposes, without restrictions on working hours or other human constraints.

In "I, Robot", *Isaac Asimov* writes: "You just can't differentiate between a robot and the very best of humans." In our view, this is not true: In some ways, robots are better. And law enforcement seems to agree, as their hope is that AI monitoring of public areas and the gathering of video footage can help in the prevention and detection of crimes as well as in the enhancement of public safety, with robots being deployed to patrol high-security areas. Robots can also be utilized in search and rescue operations, especially in hazardous environments in which human access is limited or dangerous. They can navigate debris, locate missing persons, and provide rescue teams with critical information. Robots designed for bomb disposal can be used to handle potentially explosive devices safely and defuse dangerous situations without risking human lives.

However, the benefits are accompanied by drawbacks. Two research projects have been launched to fully understand the pros and cons: at the University of Basel on "Human-Robot Interactions: Legal Blame, Criminal Law and Procedure" and at the University of Luxembourg on "Criminal Proceedings and the use of AI Output as Evidence". They do not only explore in detail the possible impact of AI on fact-finding in criminal justice but they also tackle other legal and societal concerns, including the detrimental effects on democracy when surveillance becomes a permanent feature of daily life, the lack of accountability for decisions taken by AI, and potential biases in algorithmic decision-making that can lead to discrimination.

These concerns have led to a demand for regulation, which is a complex issue. By now, several fixpoints for mitigating the risks have been identified, such as more transparency in AI systems to allow humans to better understand the decision-making process and trace bias. While regulators grapple with the construction of an adequate legal framework by which to harness the benefits of AI, they must also ensure that it is balanced with the preservation of data privacy, safety, and security.

There are many reasons why human supervision and responsibility will be key for the application of AI, with a differentiation between more or less sensitive areas. Thus, the potentially most provocative question is asked in this issue: Why do we still need a "human court" if we could use an AI-driven tool to render decisions much more cheaply, quickly, and possibly even more fairly? The answer might well be that we, as humans, want to take meaningful responsibility for decisions made on the lives of others and for shaping the society they live in. After all, we wish to avoid a future like the one described in *Alex Garland's* "Ex Machina": "AI looks back on us the same way we look at fossil skeletons on the plains of Africa. An upright ape living in dust with crude language and tools, all set for extinction."

To avoid this, the core human task persists: to understand the capabilities and limitations of technology and use it wisely based on scientific research.

Sabine Gless, Professor of Criminal Law and Criminal Proceedings at the University of Basel, Switzerland;
Katalin Ligeti, Professor of European and International Criminal Law, University of Luxembourg.

Editor's Remarks

Dear Readers,

The first eucrim issue in 2023 starts into the future with a modern, fresh design and a new subtitle on its cover. At its meeting on 17 March 2023, the editorial board agreed to change the subtitle to "European Law Forum: Prevention, Investigation, Prosecution". This change emphasises that eucrim is a project at the crossroads of European administrative law and criminal law, focusing not only on criminal law enforcement but also on concepts of preventive justice. From the very beginning, eucrim has sought to broaden the content in its news bulletins and articles beyond pure criminal law, but this was not always visible. We now hope that more and more colleagues specialised in constitutional, public, and administrative law will feel as welcome as their criminal law peers to share their views on developing new visions and models for the European cooperation and integration of the national law systems in the supra-national European context – eucrim's core mission. Today, it is no longer possible to treat administrative law and criminal law separately; the lines between legal areas are blurring. At the Union level, this has become obvious, for example, in the institutional setting for the protection of the EU's financial interests: the European Anti-Fraud Office is responsible for administrative investigations, on the one hand, and the European Public Prosecutor's Office is responsible for criminal investigations, on the other, but both bodies must closely work together. It is also true for competition law, environmental law, the market regulatory framework, and anti-money laundering measures, to name only a few. We hope that the new subtitle will make these interconnections more visible to the public and help solicit written contributions in the field of "criministrative justice".

The editorial board also unanimously agreed to keep the words "European" and "forum" in the subtitle. "European" means first and foremost that eucrim continues to cover current developments both within the European Union and also as regards the Council of Europe. Second, it reflects that eucrim covers developments both at the European (EU and CoE) level and at the national level. The deliberate choice of the word "forum" (instead of "journal" or "law review") even has four implications: First, eucrim invites both legal practitioners and academics to share their views on topical issues of European "criministrative" law. Second, we aim to strengthen intra- and interdisciplinary research into the current challenges Europe is facing. Third, the content is published online on an ongoing basis via the eucrim website (https://eucrim.eu/) as well as in a complete issue available on the website and as a hard copy. Fourth, even though explicit reference is no longer made to them in the subtitle, eucrim continues to support the national Associations on the Protection of the EU's Financial Interests/European Criminal Law by providing a platform for them to make their unique networks of practitioners and academics visible to the general public and to exchange information on their activities and projects.

The new eucrim issue also comes with a new, more colourful design for the cover, showing continuity but also underlining the new impetus and reflecting suggestions from our readership. Changes have also made on the pages inside, which feature new fonts and sans serif lettering in order to make the texts easier to read. Lastly, we adapted some titles in the news section to reflect that the news items cover current developments in both criminal law and administrative law. We have introduced a new "rule of law" category under the heading "Foundations". Up to now, news reports on recent rule-of-law developments were scattered throughout different news categories. Now, all rule-of-law developments can be found in the new category, including those on the conditionality mechanism. Similar considerations led us to establish a separate category for "Artificial Intelligence" (AI) under the section Foundations, because the impact of AI in the field of security and criminal law has become increasingly significant; this is also reflected in the guest editorial and by the selection of articles in this special issue.

Improvements to eucrim can only be made with the valuable support we gratefully receive from you as readers and users. We would like to encourage you to provide feedback using the evaluation form (available in the footer of the eucrim website under "Tools & Feedback") and to contribute to the forum by providing information on key developments in your country, by debating a hotly discussed topic, and by informing us about or reporting on an interesting conference.

We hope you enjoy reading this issue and all the issues yet to come!

The Editors of eucrim and the Members of the eucrim Editorial Board

News

Actualités / Kurzmeldungen*

European Union

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

Foundations

Fundamental Rights

Council Emphasises Civic Space in Protecting and Promoting Fundamental Rights

On 10 March 2023, the JHA Council adopted conclusions on the role of the civic space in protecting and promoting fundamental rights in the EU. The conclusions emphasise the essential role freedom of association plays in ensuring a democratic and pluralist society and the proper functioning of public life. Unjustified restrictions to the operating space of civil society organisations (CSOs) and human rights defenders can present a threat to the rule of law. Member States are called on to do the following:

- Safeguarding and promoting an enabling environment for CSOs and human rights defenders;
- Providing CSOs with a range of opportunities to cooperate;
- Taking targeted actions against threats, attacks, smear campaigns etc. against oranisations, staff and volunteers;
- Establishing the possibilities that CSOs and human rights defenders can act safely and independently in the digital space;
- Tackling challenges related to funding by ensuring fair distribution through transparent and non-discriminatory criteria;
- Ensuring meaningful participation of CSOs when legislation and policy measures are drafted and implemented.

The Commission is, *inter alia*, invited to continue providing adequate and accessible funding, simplify open calls and continue to use innovative approaches. (TW)

Rule of Law

Parliament's Assessment of Commission's 2022 Rule of Law Report

On 30 March 2023, the European Parliament voted on a resolution comprising Parliament's assessment of the Commission's 2022 rule of law report (→eucrim 3/2022, 166–167) and the overall state of EU values. MEPs welcomed improvements in the Commission's annual reporting tool but called for the scope of analysis to be expanded in order to cover the entire range of EU values. They also criticized the persistent politicisation of national councils of judiciary in some countries and the lack of country-specific recommendations regarding the illegal use of spyware by Member States. The resolution set out outstanding calls from the EP, such as the creation of a direct link between the annual rule of law reports, among other sources, and the Rule of Law Conditionality Mechanism.

Together with *Věra Jourová*, the Vice President of the Commission, the MEPs also discussed the democratic backsliding of some Member States. They noted a certain amount of regression in Greece in terms of judicial independence, corruption, and the monitoring of journalists, political rivals, and other persons of interest. As regards Spain, the MEPs discussed judicial reforms, judicial independence, and the impasse over filling positions on the national council of the judiciary. The main topics of discussion with regard to Malta were the general political climate of the nation, the fight against corruption, and the investigations and prosecutions related to the murder of investigative journalist *Daphne Caruana Galizia*. (AP)

* Unless stated otherwise, the news items in the following sections (both EU and CoE) cover the period 1 January – 30 April 2023. Have a look at the eucrim website (https://eucrim.eu), too, where the complete news items have been published beforehand.

Poland: Rule-of-Law Developments January – April 2023

This news item continues the overview of rule-of-law development in Poland (as far as they relate to Europen law) from 1 January to 30 April 2023. They follow up the last update in →eucrim 4/2022, 222–223.

■ 13/16 January 2023: The Sejm (lower house of the Polish Parliament) passes the bill "*Projekt ustawy*" and transmits it to the Senate. The bill aims to make further reforms to the disciplinary regime in the Polish judiciary in order to meet the milestones as requested by the EU institutions for receiving money from the Recovery and Resilience Facility. The bill transfers the powers of adjudicating disciplinary cases against judges of the Supreme Court, Military Courts and ordinary courts from the Chamber of Professional Liability at the Supreme Court to the Supreme Administrative Court (SAC) of Poland. The Chamber of Professional Liability was only established in June 2022 to replace the controversial Supreme Court's Disciplinary Chamber whose independence was called into question by the ECtHR and CJEU (→eucrim 2/2022, 82). In addition, the bill makes further clarifications to the disciplinary grounds, thus supplementing amendments made in June 2022 to the disciplinary grounds introduced in 2020. Accordingly, disciplinary liablity of judges would be excluded for the content of judgements or for assessments on the criteria of "a tribunal established by law" with regard to the appointment prodecures of judges.

■ 25 January 2023: The OSCE Office for Democratic Institutions and Human Rights (ODHIR) provides an opinion on the recent bill of 13 January 2023 (see above). ODHIR concludes that "the Bill introduces mechanisms to address some of the existing issues in the justice system, the efficiency and effectiveness of the proposed solution, as it is, remains doubtful." ODHIR mainly criticizes that independence and impartilality of the SAC itself is not guaranteed since it is, to a significant degree, composed of neo-judges appointed by the still flawed National Council of the Judiciary (NCJ). Moreover, broad and vague disciplinary grounds for judges have not been repealed making the disciplinary regime still subject to potential arbitrariness.

■ 6 February 2023: The Sejm's Justice and Human Rights Committee rejects amendments to the bill "*Projekt ustawy*" (see above) put forward by the Polish Senate. The Senate, *inter alia*, proposed transferring disciplinary cases on judges and other legal professions to the Criminal Chamber of the Supreme Court (instead to the Supreme Administrative Court), declaring that the rulings of the Disciplinary Chamber of the Supreme Court are invalid, and eliminating the provisions of the Muzzle Act. EU Minister *Szymon Szynkowski vel Sęk* argued that changes to the bill are impossible anymore because everything "has been accepted by the European Commission".

■ 15 February 2023: The European Commission refers Poland to the ECJ for violation of EU law by the Polish Constitutional Tribunal. The underlying infringement procedure against Poland was opened on 22 December 2021. The Commission tackles above all the Constitutional Tribunal's decisions of 14 July and 7 October 2021 in which it considered provisions of the EU Treaty incompatible with the Polish Constitution, thus questioning the primacy of EU law. According to the Commission, this case law not only infringes the general principles of autonomy, primacy, effectiveness, uniform application of Union law and the binding effect of CJEU rulings, but also Art. 19(1) TEU, which guarantees the right to effective judicial protection. Moreover, the Commission considers that the Constitutional Tribunal no longer meets the requirements of an independent and impartial tribunal previously established by law. The Polish government's was unable to dispel the Commission's concerns in the prephase of the Court proceedings.

■ 16 February 2023: The Polish Government informs the Registry of the ECtHR that Poland will not respect interim measures indicated by the ECtHR on 6 December 2022 to reinstate three Polish judges in the criminal division of the Warsaw Court of Appeal. The Polish Governement refers to a statement by *Piotr Schab*, President of the Court of Appeal in Warsaw, that "there were no factual or legal grounds for doing so". He pointed to the Constitutional Tribunal's judgment of March 2022 questioning the ECtHR's authority to intervene in cases concerning the judiciary (→eucrim 1/2022, 6). This is the first time that Poland has refused to comply with the ECtHR's interim measures in such cases.

■ 1/6 March 2023: The struggle between "old" judges and "neo-judges" at the Polish Supreme Court continues. *Małgorzata Manowska*, acting as the First President of the Supreme Court, has seemingly refused to hand over files of CJEU rulings questioning the legality of appointments of adjudicating judges by the politicised National Council of the Judiciary (NCJ). Judges at the Supreme Court further report that they are arbitrarily moved to other positions by the Court's President. In addition, Polish Minister of Justice, *Zbigniew Ziobro*, is alleged to continue his policy to install his "own people" as Presidents in Polish courts.

■ 17 March 2023: More than 1700 judges and prosecutors sign a letter defending Judge *Joanna Knobel* who acquitted 32 defendants a few days before. The defendants were indicted for their protests in the Poznán Cathedral in October 2020 against the ruling of the Polish Constitutional Tribunal tightening the abortion law. Judge Knobel was attacked for the acquittal by the Polish Minister of Justice and the president of the NCJ. The letter reacts by giving support to the decision and by defending judicial independence.

■ 23 March 2023: On the occasion of the latest developments on the Polish judiciary, a discussion takes place in the EP's Committee on Civil Liberties, Justice and Home Affairs (LIBE). The opinion of ODHIR of 25 January 2023 on the compatibility of the bill "*Projekt ustawy*" with rule-of-law standards (cf. supra) was presented. The discussion focused on the problematic politicisation of the NCJ and the growing number of judges appointed after the NCJ's reform. Justice Commissioner *Didier Reynders* expressed concern about the situation in Poland, where the decisions of the CJEU and ECtHR on independence continue to be ineffectively implemented. Regarding the Art. 7-TEU-procedure, he called for the blockade in the Council to be resolved.

■ 4/20 April 2023: The press reports that disciplinary commissioners initiated disciplinary proceedings against judges who took decisions in which they challenged the status of neo-judges at the bench applying the case law of the CJEU and ECtHR. The proceedings come despite a compromise found between the Polish government and the European Commission to reform the so-called muzzle law against Polish judges. The arrangement actually included to stop attacks against judges who apply EU law.

■ 21 April 2023: In the infringement proceedings in Case C-204/21 between the Commission and Poland, the Vice-President of the ECJ orders a reduction of the amount of the periodic penalty payment against Poland from €1 million to €500,000 per day. In October 2021, Poland was ordered to pay €1 million per day in order to give effect to interim measures set out previously in July 2021 (→eucrim 4/2021, 200 and eucrim 3/2021, 135). The measures aimed at complying with EU rule-of-law standards after the Commission brought to Court Poland's reform of the organisation of the judiciary. The reduction of the daily penalty payment takes into account that Poland meanwhile put in place certain reform measures, in particular the abolishment of the controversial Disciplinary Chamber. However, the Vice-President's order also emphasises that the measures adopted are not sufficient to ensure that all the interim measures set out in the order of 14 July 2021 have been put into effect. In addition, it is clarified that the reduction has no retroactive effect. (TW)

Hungary: Rule-of-Law Developments January – April 2023

This news item continues the overview of previous eucrim issues reporting on recent rule-of-law developments in Hungary (as far as they relate to European law). The overview follows up the one in eucrim 3/2022, 169–170.

■ 23 January 2023: In a contribution for the European Commission's 2023 rule of law report, the Hungarian Helsinki Committee (HHC) showcases the negative effects of the rule-of-law backsliding in Hungary on institutions and mechanisms crucial for a well-functioning criminal justice system. The criticism includes undermining the independence of the judiciary, governmental attacks against lawyers, and hasty legal changes without meaningful public consultation.

■ 3/21 February 2023: NGOs assess the Hungarian bill that will bring about changes to the judicial system in Hungary and which was presented in January 2023. The bill is intended to fulfil the "super milestones" concerning the judiciary, which were agreed with the EU institutions in order to unblock money from the EU's Recovery and Resilience Facility (RRF). The NGOs found that there are milestone elements the Government's proposal fully complies with, but these are mostly the ones that are rather technical in nature. At the same time, milestones that demand core changes in the judicial system remain non-implemented. In a summary table, the NGOs listed the milestones and the problems with implementation.

■ 24 February 2023: The Hungarian Helsinki Committee (HHC) explains Hungary's current legal framework of special legal order regimes and voices its concern over the prolonging governance under the state of danger. According to the HHC's paper, since 1 November 2022, the state of danger has a new constitutional and statutory basis, but these legislative changes mainly mean that problematic practices developed during the COVID-19 pandemic have been cemented by the legislature into the Hungarian legal system. The state of danger currently persists with reference to the war in Ukraine.

■ 17 April 2023: The dispute continues on whether the planned Hungarian legislative reforms concerning the judiciary fully comply with the super milestones for the sake of unfreezing RRF grants (cf. supra). The debate is specifically on the extent to which Hungary must remove the ability of public authorities to challenge final decisions of the ordinary courts before the Hungarian Constitutional Court. Such removal is required by milestone no 216. The Commission particularly criticised that allowing public authorities to file a constitutional complaint for breach of their rights undermined the right to an effective remedy of other parties as well as the right to respect the *res iudicata* character of a final judicial decision. Civil society organisations claim that the Hungarian legislature should *expressis verbis* exclude the possibility of public authorities acting in their capacity as such, to submit a constitutional complaint before the Constitutional Court, which has not been done so far.

■ 22 April 2023: Hungary's President *Katalin Novák* vetoes a parliamentary act that would enable people to report on those who challenge the "constitutionally recognized role of marriage and the family" and those who contest children's rights "to an identity appropriate to their sex at birth." In particular, citizens would have been enabled

to anonymously report same-sex couples raising children together. The law was criticised for being discriminatory toward LGBTQ+. This is the first time that a head of state had objected to a law of great importance to *Victor Orbán's* ultra-conservative ideology since the right-wing populist Prime Minister came into office in 2010.

■ 25 April 2023: Hungarian civil society organisations present a full assessment of the steps taken by the Hungarian Government to comply with the milestones established by the EU institutions to access EU funds (cf. supra). According to the assessment, numerous issues related to the anti-corruption framework, competition in public procurement, judicial independence, the predictability, quality and transparency of law-making, the rights of refugees and asylum-seekers, academic freedom and the rights of LGBTQI+ persons remain unresolved, and remedial measures taken so far remain unsatisfactory.

■ 3 May 2023: The Hungarian parliament passes an act that entails judicial reforms. The reform is designed to meet the four super milestones on the judiciary (cf. supra). The act strengthens the powers and role of the National Judicial Council, reinforces the independence of Hungary's Supreme Court (Kúria), abolishes the power of public authorities to lodge constitutional complaints (see above), and removes obstacles to references for preliminary rulings to the ECJ. It is now up to the Commission to endorse whether the reforms can unlock EU money. Observers believe that Hungary can now have access to over €13.2 billion in EU funds. (TW)

Ukraine Conflict

EU Reactions to Russian War against Ukraine: Overview January 2023 – June 2023

This news item continues the reporting on key EU reactions following the Russian invasion of Ukraine on 24 February 2022: the impact of the invasion on the EU's internal security policy, on criminal law, and on the protection of the EU's financial interests. The following overview covers the period from the beginning of January 2023 to the end of June 2023. For overviews of the developments from February 2022 to mid-July 2022 → eucrim 2/2022, 74–80; for the developments from the end of July 2022 to the end of October 2022 → eucrim 3/2022, 170–171; for the developments from November 2022 to December 2022 →eucrim 4/2022, 226–228.

■ 17 January 2023: The European Commission publishes an update of „Frequently Asked Questions" in relation to the prohibition to provide services to the Russian government and legal persons in Russia. They relate to Article 5n of Council Regulation 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, which was considerably amended by Council Regulation 2022/1904. The amendment was introduced following the eight package of sanctions against Russia (→eucrim 3/2022, 171). It expands the ban to provide services, such as IT consultancy and legal advisory. Bars of lawyers particularly see the ban for legal advisory critically (see also below).

■ 19 January 2023: The European Parliament adopts a resolution on the establishment of a tribunal on the crime of aggression against Ukraine. The International Criminal Court (ICC) cannot currently investigate the crime of aggression when it comes to Ukraine. The MEPs therefore urge the EU, in close cooperation with Ukraine and the international community, to push for the creation of a special international tribunal to prosecute Russia's political and military leadership and its allies. This special international tribunal must have jurisdiction to investigate not only *Vladimir Putin* and the political and military leadership of Russia, but also *Aliaksandr Lukashenka* and his cronies in Belarus. In the MEPs' opinion, the creation of a special tribunal would send a very strong message to both Russian society and the international community that President *Putin* and the Russian government as a whole are subject to prosecution for the crime of aggression in Ukraine.

■ 27 January 2023: The Council decides to prolong by six months (until 31 July 2023) the restrictive measures targeting specific sectors of the economy of the Russian Federation in reaction to the military aggression against Ukraine.

■ 27 January 2023: At the informal JHA Council meeting in Stockholm, the ministers of justice discuss the crimes committed in Ukraine under international law and possibilities of dealing with them under criminal law, both with regard to the establishment of a special tribunal for Ukraine and the setting up of a provisional international prosecution authority. In this context, Eurojust informs of a new evidence database (see below). This will enable the collection, preservation and transfer of evidence relating to the core crimes of international criminal law to the competent national and international judicial authorities, including the International Criminal Court based in The Hague. The meeting was also attended by the *Denys Maliuska*, Minister of Justice of Ukraine, who reported on the current state of affairs in Ukraine.

■ 2 February 2023: Aiming at providing necessary non-lethal equipment and supplies as well as services to back training activities in Ukraine, the Council adopts assistance measures under the European Peace Facility (EPF) providing further military assistance to the armed forces of Ukraine. These consist of a seventh package worth €500 million and a new €45 million assistance measure to support the training efforts of the European Union Military Assis-

tance Mission in support of Ukraine (EUMAM Ukraine). This brings the total EU contribution for Ukraine under the EPF to €3.6 billion.

■ 3 February 2023: The 24th EU-Ukraine summit, the first summit since the start of the Russian aggression, takes place in Kyiv. On this occasion, *Charles Michel*, President of the European Council, and *Ursula von der Leyen*, President of the European Commission, meet with *Volodymyr Zelenskyy*, President of Ukraine. Among other things, they discussed Ukraine's path in Europe and the accession of Ukraine to the European Union, the EU's response to Russia's war of aggression against Ukraine, Ukraine's initiatives for just peace and accountability, etc. In a joint statement, the leaders reiterate the EU's unwavering support of and commitment to Ukraine's independence, sovereignty, and territorial integrity within its internationally recognised borders. Additionally, they denounce Russia's routine deployment of missiles and drones to target civilians, civilian property, and civilian infrastructure throughout Ukraine, which is in violation of international humanitarian law. They reaffirm that the EU will continue to provide and coordinate the full range of humanitarian assistance to and support for Ukrainian society. In order to ensure accountability for the perpetrators of international crimes, they renew their support for investigations by the Prosecutor of the International Criminal Court. Furthermore, they express their support for the establishment of an International Centre for the Prosecution of the Crime of Aggression in Ukraine (ICPA) in The Hague. This centre would be linked to the existing Joint Investigation Team supported by Eurojust (→eucrim 2/2022, 79–80).

■ 4 February 2023: The Council sets two price caps for petroleum products falling under CN code 2710, which originate in or are exported from Russia. The first price cap for petroleum products traded at a discount to crude oil is set at $45 per barrel, while the second price cap for petroleum products traded at a premium to crude oil is set at $100 per barrel.

■ 9 February 2023: The heads of state and government hold a special meeting of the European Council. In their summit conclusions, they reaffirm the commitments already expressed and taken up in the joint statement issued after the 24th EU-Ukraine Summit of 3 February 2023. They repeat their resolute condemnation of Russia's war of aggression against Ukraine and their commitment in holding accountable all commanders, perpetrators, and accomplices of war crimes and other most serious crimes committed in connection with the war. The support for establishing an appropriate mechanism for the prosecution of the crime of aggression is underpinned. The European Council also reaffirms the continuous financial support to Ukraine and its people which so far amounts to at least €67 billion.

■ 15 February 2023: The Committee of Permanent Representatives of the Member States decides to set up an *ad hoc* working group on the use of frozen Russian assets for reconstruction in Ukraine. The working group is to be chaired by *Anders Ahnlid*, Swedish Ambassador to the EU, and mandated to conduct a comprehensive legal, financial, economic and political analysis of the possibilities of using frozen Russian assets. The group will work closely with the „Freeze and Seize Task Force", which the Commission already established in March 2022 (→eucrim 2/2022, 76–77).

■ 20 February 2023: The actions before the General Court to annul the ban on the provision of legal services in the EU's 8th Sanctions Package against Russia are published in the Official Journal C-63, 61–62 (→separate news item, pp. 9–10).

■ 23 February 2023: Eurojust gives an overview of its support to the judicial response to alleged core international crimes committed in Ukraine. It presents the newly established Core International Crimes Evidence Database (CICED) and updates on the setting up of the new International Centre for Prosecution of the Crime of Aggression against Ukraine (→separate news item, p. 11).

■ 25 February 2023: The Council adopts the 10th package of economic and individual sanctions, imposing further export bans on critical, technological, and industrial goods (such as electronics, machine parts, spare parts for trucks and jet engines, etc.) to the Russian Federation. The 10th package also targets dual use goods, e.g. pyrotechnic articles that can have a dual military and commercial use. The transit through Russia of EU-exported dual use goods and technology is prohibited. The package expands the list of individual entities directly supporting Russia's military and industrial complex in its war of aggression by an additional 96 entities. Taking into account the direct connection between Iranian manufacturers of unmanned aerial vehicles and the Russian military and industrial complex as well as the concrete risk that certain goods or technology are used for the manufacture of military systems contributing to Russia's war against Ukraine, this list includes seven Iranian entities for the first time. Addressing Russia's systematic campaign of disinformation, the Council added two additional media outlets to the list, suspending their broadcasting licences: RT Arabic and Sputnik Arabic. Moreover, the Council introduces more detailed reporting obligations for funds and economic resources belonging to listed individuals and entities that have been frozen or were subject to any move shortly before the listing. The list of entities subject to the asset freeze and the ban on releasing money and other resources for the economy now includes three Russian banks. Altogether, EU's restrictive measures in respect of the

war in Ukraine now apply to a total of 1 473 individuals and 205 entities.

■ 8 March 2023: The General Court decides to annul the restrictive measures applied to Ms *Violette Prigozhina*, mother of Mr *Yevgeniy Prigozhin*. The latter is responsible for the deployment of Wagner Group mercenaries in Ukraine in the context of Russia's war against Ukraine. (→separate news item, p. 9).

■ 9/10 March 2023: At the JHA Council meeting, the justice and home affairs ministers of the EU Member States discuss internal security issues and judicial responses in relation to Russia's war of aggression in Ukraine. The importance of CSDP missions for advice and capacity building in Ukraine is underlined and closer cooperation between these missions and the JHA area envisaged. An update is given on actions taken by national authorities and at the EU level to fight impunity of crimes committed in connection with Russia's aggression.

■ 13 March 2023: The Council prolongs restrictive measures targeting 1473 individuals and 205 entities responsible for undermining or threatening the territorial integrity, sovereignty, and independence of Ukraine for another six months (until 15 September 2023).

■ 20 March 2023: Responding to Ukraine's urgent needs, the Council agrees on a three-track approach with the aim, in particular, of speeding up delivery and joint procurement, aiming at one million rounds of artillery ammunition for Ukraine. This is a joint effort over the next twelve months and calls for swift implementation.

■ 23 March 2023: The President of Ukraine, *Volodymyr Zelenskyy* joins the European Council's meeting via video conference. EU leaders welcome a resolution by the UN General Assembly on „Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine", which was adopted with broad support from the international community. Support for President *Zelenskyy*'s peace plan is also given. The European Council takes note of the arrest warrants against Russia's President and his Commissioner for Children's Rights recently issued by the International Criminal Court for the war crime of unlawful deportation and transfer of Ukrainian children from occupied areas of Ukraine to Russia. It also acknowledges Ukraine's commitment and reform efforts, underlining the importance of Ukraine's EU accession process. Again, the agreement to create the new International Centre for Prosecution of the Crime of Aggression against Ukraine (ICPA) in The Hague is welcomed. Possible further restrictive measures and efforts towards the use of Russia's frozen assets for the reconstruction of Ukraine are discussed.

■ 30 March 2023: The EU JHA agencies publish an updated overview of their activities to support the Ukraine after the start of the Russian invasion in February 2022 (→separate news item, p. 10).

■ 13 April 2023: The Council adds the Wagner Group, a Russia-based unincorporated private military entity established in 2014, and RIA FAN, a Russian news agency, to the list of those subject to EU restrictive measures for actions that undermine or threaten the territorial integrity, sovereignty and independence of Ukraine. While the Wagner Group is actively participating in the Russian war of aggression against Ukraine and spearheaded the attacks against the Ukrainian towns of Soledar and Bakhmut, RIA FAN is involved in pro-government propaganda and disinformation on Russia's war against Ukraine.

■ 13 April 2023: As part of the Council agreement of 20 March 2023 on a three-track approach intended to speed up the delivery and joint procurement of artillery ammunition, the Council adopts an assistance measure worth €1 billion under the European Peace Facility (EPF) to support the Ukrainian Armed Forces. This measure allows the EU to reimburse Member States for ammunition donated to Ukraine between 9 February and 31 May 2023.

■ 24 April 2023: The Foreign Affairs Council exchange views on the Russian aggression against Ukraine. The discussion starts with a briefing by the Foreign Minister of Ukraine, *Dmytro Kuleba*, addressing EU ministers on the latest developments on the ground and Ukraine's military priorities and needs, especially in terms of ammunition and missiles. During the discussion, *Josep Borrell*, High Representative for Foreign Affairs and Security Policy, stress that the EU and its Member States have facilitated the delivery of over €13 billion in military support. He updates ministers on the EU's military support to Ukraine in the context of the three-track plan to provide Ukraine with one million rounds of artillery ammunition. The Foreign Affairs Council then discusses the implementation of the EU action plan on the geopolitical consequences of the Russian aggression. Due to instability brought by the Russian war in Ukraine and a fragmented geopolitical context, the EU aims to strengthen its partnerships around the world, based on political and economic engagement and mutual cooperation.

■ 25 May 2023: The Council adopts a Regulation on temporary trade liberalisation supplementing trade concessions applicable to Ukrainian products. In order to maintain the stability of Ukraine's trade relations with the EU and keep its economy going under very challenging circumstances, the Regulation renews the suspension of all customs duties, quotas, and trade defence measures on Ukrainian exports to the EU for another year (until June 2024). The regulation concerns all outstanding customs duties under Title IV of the Association Agreement

between the EU and Ukraine establishing an in-depth and comprehensive free trade area (DCFTA), the collection of anti-dumping duties on imports originating in Ukraine as of the date of entry into force of this Regulation, and the application of the common rules for imports (safeguards) with respect to imports originating in Ukraine. The Regulation enters into force on 6 June 2023.

■ 9 June 2023: The Council agrees on a general approach for the draft EU Directive on the definition of criminal offences and penalties for the violation of Union restrictive measures. Compared to the Commission proposal of 2 December 2022 (→eucrim 4/2022, 225), the Council's approach strengthens the definition of offences that need to be criminalised, tightens the penalties, which must be effective, proportionate and dissuasive in the Member States, and advocates stricter enforcement. The general approach is the basis for entering into interinstitutional negotiations with the European Parliament. The new EU legislation aims to ensure that EU's restrictive measures against persons who support Russia's war of aggression in Ukraine are fully implemented and violation of these measures will be subject to deterrent effects.

■ 23 June 2023: The Council adopts the 11th package of economic and individual sanctions in view of Russia's aggression of war in Ukraine. The actions, among other things, strengthen bilateral and multilateral cooperation with third countries to impede sanctions' circumvention, prohibit the transit of goods and technology via Russia, tighten export restrictions (particularly in relation to dual use goods and technology), and further suspend licences of media outlets involved in disinformation campaigns. Furthermore, the EU imposes restrictive measures on an additional 71 individuals and 33 entities responsible for actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. In this context, the Council extended the existing listing criterion on circumvention and adopted the first listing related to sanctions circumvention. In response to the information warfare conducted by Russia, a new listing criterion to cover companies in the IT sector that provide critical technology and software to the Russian intelligence community is introduced as well; this led to first listings of IT companies in this respect. Other designations include officials and companies active in the Russian military and defence sector, individuals responsible for the forced transfers and deportation of Ukrainian children, persons responsible for the looting of Ukraine's cultural heritage, and actors involved in disinformation. Lastly, also members of the judiciary who took politically motivated decisions against Ukrainian citizens who opposed the annexation of Crimea, as well as businesspersons, a deputy minister and a number of Russian local officials and two banks are put on the list. The EU's restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine now apply to almost 1800 individuals and entities altogether. (AP/TW)

Annulment of Restrictive Measures Applied to Mother of Wagner Group Founder

On 8 March 2023, the General Court decided to annul the restrictive measures applied to Ms *Violetta Prigozhina*, mother of Mr *Yevgeniy Prigozhin*, who is responsible for the deployment of Wagner Group mercenaries in Ukraine in the context of Russia's war against Ukraine.

The Council had adopted a series of restrictive measures on 17 March 2014 in response to the illegal annexation of Crimea and the city of Sevastopol by Russia in March 2014 and in response to Russia's destabilising actions in eastern Ukraine. The restrictive measures were directed against certain persons responsible for actions or policies that undermine or threaten the territorial integrity, sovereignty, and independence of Ukraine and against persons, entities, or bodies associated with them.

After Russia's war against Ukraine began in February 2022, the Council, in its acts of 23 February 2022, added more persons to the lists of those subject to restrictive measures. In this context, it added Ms Violetta Prigozhina's name as the owner of different undertakings with links to her son, Yevgeniy Prigozhin, and therefore supporting actions and policies that undermine the territorial integrity, sovereignty, and independence of Ukraine.

On 21 April 2022, Ms Prigozhina brought an action against the application of the restrictive measures before the CJEU and requested annulment of the contested act. The General Court granted her request, remarking that the link establishing an association between the two persons at the time of the adoption of the contested acts is based solely on their family relationship. According to the judges in Luxembourg, this is not sufficient to justify the mother's inclusion on the contested lists. An appeal, limited to points of law only, may be filed with the ECJ within two months and ten days of being notified of the decision. (AP)

Actions against Ban on Legal Advisory Services in 8th Sanctions Package

On 20 February 2023, the actions brought by the *Ordre néerlandais des avocats du barreau de Bruxelles and Others v Council* (reference: Case T-797/22) and by the *Ordre des avocats à la cour de Paris and Couturier v Council* (reference: Case T-798/22) against the ban on legal advisory services contained in the EU's 8th sanc-

tions package against Russia were published in the EU's Official Journal. The Council adopted the 8th package of sanctions for Russia's continued aggression against Ukraine on 6 October 2022 (→eucrim 3/2022, 171). Both actions before the General Court seek to achieve the following:

- Annulment of Art. 1(12) of Council Regulation (EU) 2022/1904 of 6 October 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine;
- Annulment of Art. 1(13) of Council Regulation (EU) 2022/2474 of 16 December 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

The *Ordre néerlandais des avocats du barreau de Bruxelles and Others* claim that the general prohibition on the provision of legal advisory services infringes on Arts. 7 and 47 CFR. They further allege a breach of the principle of proportionality, as the introduction of a general prohibition on the provision of legal advisory services is not viewed as suitable for achieving the legitimate objectives pursued by the EU in the context of the conflict between Russia and Ukraine. They claim a general prohibition goes beyond what is strictly necessary to achieve those objectives. Lastly, the applicants consider a breach of the principle of legal certainty.

The *Ordre des avocats à la cour de Paris and Couturier* claim an infringement of the obligation to state reasons as laid down in Art. 296 TFEU by the general prohibition on the provision of legal advisory services. They argue that the Council provides no explanation as to the reason for the general prohibition on the provision of legal advisory services in non-contentious matters. They further allege an infringement of the legal professional privilege of the lawyer and of the right to be „counselled" by a lawyer. (AP)

Update on JHAAN Joint Paper on Solidarity with Ukraine

On 30 March 2023, the network of the EU Justice and Home Affairs Agencies (JHAAN) published an update of the joint paper on its contribution to the EU's solidarity with Ukraine (for the initial paper →eucrim news of 14 October 2022). The update sets out the main activities of the agencies in the period from February 2022 to February 2023 in their effort to support EU Member States and institutions in response to Russia's military aggression against Ukraine and to help people affected and displaced by the war.

The activities of the agencies during this period include the following:

- Producing targeted analytical products and reports;
- Identifying key fundamental rights challenges and ways to overcome them;
- Providing operational support to investigations into core international crimes allegedly committed in Ukraine;
- Providing operational support to national authorities, with a particular emphasis on Member States bordering Ukraine and Moldova;
- Providing information on provision-related activities and support;

Study on Impact of International Sanctions on Russian Oil Exports

In an article published on 22 February 2023, researchers *(T. Babina, B. Hilgenstock, O. Itskhoki, M. Mironov, and E. Ribakova)* assessed the impact of international sanctions on Russian oil exports. They focused on the EU's embargo on seaborne crude oil and the Group of Seven's (G7) price cap mechanism, both having taken effect on 5 December 2022. The paper established four key findings:

- In 2022, Russia's exports of products hit a record $532 billion, resulting in an all-time high trade surplus of $316 billion, due to the fact that sanctions on Russian energy were only put in place toward the end of the year;
- Without sacrificing volume, Russia was able to divert crude oil exports from Europe to substitute markets like India, China, and Turkey, but at the cost of giving discounts in some of the areas in which the EU embargo has significantly reduced demand (i.e. shipments from Baltic and Black Sea ports);
- The crude oil discounts were not as significant as those indicated in Urals prices: based on the data, the average export price for Russian crude oil stood at about $74 per barrel in the post-embargo/price cap period against Urals at $52 per barrel;
- Russian oil exports from Pacific Ocean ports do not comply with the G7 price cap. The 50% shipments of oil, which are not transported via *Sovcomflot* or the *shadow fleet*, should be subject to the cap, as they involve Western shipping services.

The study put forth three policy recommendations:

- The sanctions on Russian oil exports should not be abolished, as the EU embargo on Russian oil played a key role in driving the deep discounts on Russian oil. The enforcement of sanctions on Russian oil exports, including ensuring compliance with price cap-related restrictions on shipping, maritime insurance, and other services is crucial;
- The fact that a sizeable portion of Russian crude oil is being sold considerably over the $60/barrel price ceiling level urgently requires additional scrutiny of these transactions and reinforces the need for increased enforcement;
- The price caps on crude oil should be lowered as soon as possible. As the post- embargo period has demonstrated, Russia is willing to accept lower prices on some of its shipments and is unlikely to cut volumes as long as the price cap level remains above production costs. A lower cap could therefore significantly impact Russia's earnings from crude oil exports. (AP)

- Contributing to the enforcement of EU sanctions;
- Supporting the authorities of Ukraine and Moldova.

The update was prepared by the European Union Agency of Asylum (EUAA), which holds the Presidency of the JHAAN in 2023. Agencies of the JHAAN include CEPOL, EIGE, EMCDDA, EUAA, eu-LISA, Eurojust, Europol, FRA, and Frontex. (CR)

Eurojust Launches Core International Crimes Evidence Database and Gives Overview of Judicial Support for Ukraine

One year after the start of the war in Ukraine, Eurojust and its partners looked back on a range of measures and actions to support the judicial response to alleged core international crimes. In addition to the review, Eurojust updated about the following:

On 23 February 2023, the newly established Core International Crimes Evidence Database (CICED) began operation. CICED is a tailor-made, centralised judicial database set up by Eurojust to preserve, store, and analyse evidence of core international crimes in a secure mode. With the help of the CICED, systematic actions behind core international crimes shall be made identifiable and, in this way, help advance national and international investigations, thereby ensuring that efforts are not duplicated. The CICED consists of three components: a safe digital data transmission method, secure data storage, and advanced analysis tools.

The database also contains a register of information on who submitted the evidence as well as the event and type of crime being referred to. Evidence can only be submitted by competent national authorities from EU Member States and countries with Liaison Prosecutors at Eurojust. The submission of evidence is voluntary, and it is not shared without the permission of the submitting authority. A factsheet on the CICED is available here.

In addition, Eurojust is in the process of setting up a new International Centre for Prosecution of the Crime of Aggression against Ukraine (ICPA). The aim of the centre will be to support and enhance investigations into the crime of aggression by securing key evidence and facilitating case building at the earliest possible stage. The centre will become an integral part of the existing support structure for the Joint Investigation Team (JIT) on Ukraine at Eurojust (see below), with Eurojust providing legal, operational, and logistic support. The centre was announced by European Commission President *Ursula von der Leyen* at a joint press conference with Ukrainian President *Zelensky* on 2 February 2023. It was made official at the United for Justice Conference that took place on 3–5 March 2023 in Ukraine.

At the conference, the ICPA officially joined the JIT agreement on alleged core international crimes committed in Ukraine that was signed on 25 March 2022 by Lithuania, Poland, and Ukraine. Estonia, Latvia, Slovakia, and Romania as well as the ICC have since joined (→eucrim news of 21 June 2022). In support of this JIT, Eurojust provided legal, logistical, financial, and analytical support and hosted 14 coordination meetings over the last 12 months. On 3 March 2023, the seven national authorities participating in the JIT also signed a Memorandum of Understanding (MoU) with the United States Department of Justice. The MoU enhances coordination between the partner countries and the US authorities regarding investigations in connection with the war in Ukraine.

To keep track of Eurojust's role in the judicial proceedings with regard to the war in Ukraine, a dedicated webpage includes the latest developments, press releases, tweets, and videos. The webpage can be found here. (CR)

Schengen

Upgraded Schengen Information System Went Live

On 7 March 2023, the renewed Schengen Information System (SIS) was launched and became fully operational. Law enforcement authorities in 30 European countries are now able to enter and see new categories of alerts and share more data. The legal bases for the upgraded SIS was already laid in 2018 (→eucrim 4/2018, 192–193), but it took until now to put the legal provisions into operation ("SIS 3.0"). The main new features of the SIS include:

- In addition to photographs and fingerprints, the SIS will contain new types of biometrics, e.g., palm prints, fingermarks and palmmarks, as well as DNA records (but only in relation to missing persons), so that persons sought can be more easily located and identified;
- New inquiry check alerts will allow to collect targeted information on suspects of serious crime or terrorism. There will be alerts on "unknown wanted persons" containing only the prints of unknown perpetrators that are discovered at the scenes of terrorist offences or serious crime;
- In addition to existing alerts on missing persons, national authorities will be able to issue preventive alerts in the system to protect people in need (children at risk of abduction or potential victims of terrorism, trafficking in human beings, gender-based violence, or armed conflict/hostilities);
- With a view to better prevent and deter irregular migration, a new alert on return decisions allows national authorities to verify if third-country nationals have the legal right to stay in the EU. SIS will also contain data on falsified documents, including travel documents and visa stickers;
- Access rights are expanded, i.e. Europol and national immigration authorities now have access to all alert

categories in SIS. Full access by Frontex's teams will follow.

The SIS is the most widely used security database in Europe. It contains more than 90 million data sets. In 2022 alone, competent authorities consulted the SIS almost 35 million times a day. An alert entered in SIS by one country becomes available in real time in all other countries that use SIS, so that competent authorities across the EU can find the alert. (TW)

Security Union

New EU Cyber Solidarity Act Proposed

On 18 April 2023, the Commission adopted a proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services and presented a Cybersecurity Skills Academy.

With the EU Cyber Solidarity Act, the Commission aims to strengthen the capacity to detect, prepare for, and respond to significant and large-scale cybersecurity threats and attacks in the EU by creating a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism. The European Cybersecurity Shield, a pan-European infrastructure consisting of national and cross-border Security Operations Centres (SOCs) across the EU, will detect and respond to cyber threats using artificial intelligence (AI) data analysis. The Cyber Emergency Mechanism will increase preparedness and improve incident response capabilities in the EU. Both could be operational by 2024.

With the EU Cybersecurity Skills Academy, the Commission aims to close the cybersecurity talent gap by bringing together private and public initiatives and providing training and certification for interested citizens in a single online location.

The proposed regulation will now be examined by the European Parliament and the Council. (AP)

New CERIS Newsletter for Security Research in the EU

On 4 April 2023, the platform Community for European Research and Innovation for Security (CERIS) managed by the Directorate-General for Migration and Home Affairs (DG HOME) launched a newsletter on its activities. The CERIS platform facilitates interactions within the security research community and among users of research results by bringing together nearly 2000 policy makers, security practitioners, and researchers as well as representatives from academia, civil society, and industry from across Europe. With the newsletter, CERIS aims to address a specific interest in security research news. (AP)

Artificial Intelligence

The Impact of ChatGPT on Law Enforcement

spot light

At the end of March 2023, Europol's Innovation Lab published a new Tech Watch Flash Report looking at Large Language Models (LLMs), such as ChatGPT, and their impact on law enforcement. The report is based on the results of dedicated expert workshops in which the behaviour of an LLM, namely ChatGPT, was tested when confronted with potentially criminal cases of malicious use.

ChatGPT (in the GPT-3.5 version) is capable of processing and generating human-like text in response to user prompts. It can answer questions on a variety of topics, translate text, engage in conversational exchanges, and summarise text to provide key points. It is capable of performing sentiment analysis, generating text based on a given prompt (i.e. writing a story or poem), as well as explaining, producing, and improving code in some of the most common programming languages (Python, Java, C++, JavaScript, PHP, Ruby, HTML, CSS, SQL). Although several safety features were included in ChatGPT, with a view to preventing malicious use of the model by its users, the report shows that these safeguards can be circumvented. The process of refining the precise way a question is asked in order to influence the output generated by an AI system (so-called prompt engineering) can also be used to set these safeguards aside.

As for its criminal use, in particular, the report finds that ChatGPT can be used to better understand and subsequently carry out various types of crime. It offers new opportunities, especially for crimes involving social engineering, phishing, and online fraud as well as way to generate propaganda, disinformation, and fake news. Its capability of producing code makes ChatGPT a viable tool for malicious actors to create malware and other assistance to cybercriminal purposes.

From the impression of the real impact that LLMs already have and their rapid growth and further improvement, the report strongly underlines the need for law enforcement to understand this impact and be in a position to anticipate and prevent abuse. To this end, Europol also offers a more in-depth report for law enforcement only. (CR) ■

FRA Report on Use of AI in Predictive Policing and Offensive Speech Detection

spot light

On 8 Dezember 2022, the European Union Agency for Fundamental Rights (FRA) published its report on the use of artificial intelligence (AI) in predictive policing and offensive speech detection. The report took a closer look at the possible bias in algorithms that can amplify over time and affect people's lives, potentially leading to discrimination. The FRA stressed that the question on bias of algorithms is still underresearched

and evidence-based assessments are lacking. The two „use cases" on (faulty) crime predictions and (legitimate) content posted online should contribute to fill this gap. The FRA makes six recommendations:

- The quality of training data and other sources influencing bias need to be assessed by users of predictive algorithms. Using data based on outputs of algorithmic systems becomes the basis for updated algorithms, which might amplify the bias over time. With regard to predictive policing, this means that an assessment needs to be made before and during the use of algorithm.
- Additional implementing guidance on the collection of sensitive data under Art. 10 (5) of the proposed Artificial Intelligence Act should be considered, notably with respect to the use of proxies and to outline protected grounds (such as ethnic origin or sexual orientation).
- Increased transparency and assessments of algorithms are required as the first step when safeguarding against discrimination. Companies and public bodies using speech detection should be required to share the information necessary to assess bias, with relevant oversight bodies and – to the extent possible – with the public. When exercising their mandates, oversight entities responsible for upholding fundamental rights, such as equality commissions and data protection authorities, should pay special attention to the potential discrimination in language-based prediction models.
- Given that speech algorithms include strong bias against persons based on several different characteristics (such as ethnic origin, gender, religion, and sexual orientation), the EU legislator and Member States should strive to ensure consistent and high levels of protection against discrimination on all grounds. This discrimination is to be tackled by applying existing laws that safeguard fundamental rights. Existing data protection laws must also be used to ensure non-discrimination when algorithms are used for decision-making. Equality bodies should employ specialised staff and cooperate with data protection authorities and other relevant oversight bodies in order to step up their efforts to address discrimination complaints and cases linked to the use of algorithms.
- The EU and its Member States need to consider measures fostering greater language diversity in Natural Language Processing (NLP) tools as a way of mitigating bias in algorithms and improving the accuracy of data. As a first step, this should include promoting and funding NLP research on a range of EU languages other than English in order to promote the use of properly tested, documented, and maintained language tools for all official EU languages. The EU and its Member States should also consider building a repository of data for bias testing in NLP.
- An increase in EU and national funding for fundamental rights assessments of current software and algorithms is required for studies of the available, general-purpose algorithms in order to increase the deployment of trustworthy AI that complies with fundamental rights. The EU and its Member States could improve access to data and data infrastructures when identifying and combating the risk of bias in algorithmic systems by ensuring access to data infrastructures for EU-based researchers. Investments in storage and cloud computing infrastructures that meet EU criteria for data protection, software security, and energy efficiency would help to achieve this.

FRA's report aims to inform policymakers, human rights practitioners and the general public about risk of bias when using AI. It particularly feeds into the discussion on the proposed Artificial Intelligence Act (→eucrim 2/2021, 77). Here, the question on the protection of fundamental rights plays an important role. (AP) ■

Legislation

Discussion and Criticism of Proposal to Prevent and Combat Child Sexual Abuse

On 19 May 2023, the European Parliament's rapporteur *Javier Zarzalejos* published a draft report on the controversial Commission proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (COM (2022) 0209 →eucrim 2/2022, 91–92). *Zarzalejos* did not propose any substantial changes and wholly welcomed the European Commission's proposal. He supports the approach based on the assessment conducted by each provider of the risks of their services being misused for the purpose of child sexual abuse. *Zarzalejos* pointed out that the set of safeguards introduced in the proposal and the EDPB-EDPS Joint Opinion 04/2022 represented a major contribution to his assessment. Furthermore, he advocated the controversial possibility for providers to process metadata that can detect suspicious patterns of behaviour, even in the case of end-to-end encryption. The report endorsed the creation of the EU Centre on Child Sexual Abuse and proposed setting up a Victims' Consultation Forum in order to strengthen the position of victims.

Meanwhile, the European Parliament's Research Service raised concerns about the privacy and technical implications of the draft law in a complementary impact assessment published in April 2023. The study concluded that the overall effectiveness of the proposal is expected to be limited due to several factors. For example, perpetrators who wish to continue

their activities without being targeted by the measure introduced by the proposal are likely to resort to the dark and deep web, where identification is more difficult. The analysis also calls into question end-to-end encryption, because there is currently no technological solution that would allow for scanning of the confidential communications required by warrants without jeopardizing end-to-end encryption. The evaluation also made clear that the proposal would interfere with Articles 7 and 8 of the EU Charter of Fundamental Rights by violating the prohibition of general data retention and the prohibition of general surveillance obligations. While the proposal would generally benefit the protection of children, it would interfere with the fundamental rights of service users, which would not be justified. These criticisms echo those voiced by civil society and, more recently, by the German Bar Association. (AP)

First Designations under the Digital Services Act

Following the entry into force of the Digital Services Act (DSA) (→eucrim 4/2020, 273–274 and eucrim 4/22, 228–230) in mid-November 2022, the Commission adopted the first designation under the DSA on 25 April 2023. The following platforms are affected:

- Seventeen Very Large Online Platforms (VLOPs) – including Amazon Store, Apple AppStore, Facebook, TikTok, Twitter, Wikipedia, etc.;
- Two Very Large Online Search Engines (VLOSEs) – Bing and Google Search.

They each reach at least 45 million active users monthly. These companies will have four months from designation to comply with the DSA's set of obligations. The DSA aims to empower users, better protect minors, increase transparency and accountability, and ensure more careful content moderation. Designated companies will also have to report their first annual risk assessment to the Commission. (AP)

Regulation Implementing the Digital Markets Act (DMA)

On 14 April 2023, the Commission published the Regulation implementing its Digital Markets Act (DMA). The Regulation details procedural aspects related to the implementation and enforcement of the DMA, which entered into force on 1 November 2022 and become applicable on 2 May 2023, e.g. the parties' right to be heard and have file access. It intends to promote effective proceedings and give the involved companies, including those appointed as gatekeepers, legal certainty regarding procedural rights and obligations. The DMA is an EU regulatory tool that comprehensively regulates the gatekeeper power of the largest digital companies in order to make the markets in the digital sector fairer and more contestable (→eucrim 4/2022, 228–230). (AP)

Institutions

Court of Justice of the European Union (CJEU)**

Rules of Procedures of General Court Amended

On 1 April 2023, significant amendments to the Rules of Procedure of the General Court of the EU came into force. Their aim is to clarify, supplement, and simplify provisions. In addition to the revised Rules of Procedure, the General Court also amended its Practice Rules for the Implementation of its Rules of Procedure.

Now that the General Court has adopted a legal and technical framework for this purpose, videoconferencing can be used for hearings. The newly created document „Practical recommendations for representatives making oral submissions by videoconference" further assists parties' representatives in this regard. Additionally, the rules now allow for judgements and orders of the General Court to be signed electronically. The rules specify the terms for the qualified electronic signature and the rules for long-term secure storage of original electronic versions of these documents.

In the context of proactive case management, the new rules also offer new guarantees for so-called pilot cases (i.e. in pending cases raising the same issue of law, one of these cases is to be identified as the pilot case and the others are stayed). This means the pilot case will be given priority over stayed cases, which will be heard once they are resumed. Furthermore, the General Court may now organise joint hearings of two or more cases when there are similarities between them, irrespective of whether the conditions for joinder are met or not.

In the area of data protection, the Rules of Procedure now clearly distinguish between the processing of personal data of natural persons and the processing of data that is not personal data. Lastly, the General Court has introduced a new document (Provision of indicative model applications) to assist parties' representatives in preparing their actions, and it has updated the

** With this issue, we are changing the abbreviations used for the **C**ourt of **J**ustice of the **E**uropean **U**nion. In the past, we used the abbreviation "CJEU" for *both* the institution and the judgments of the Court of Justice; we will now use "CJEU" only if we are referring to the institution as such or the Court in a wider, general sense. In order to better reflect that the "CJEU" actually consists of two courts – the Court of Justice and the General Court – we will use different abbreviations when we refer to judgments/decisions of these courts. If we report on a judgment that is handed down by the Court of Justice, e.g. in references for preliminary rulings and in actions for failure to fulfil obligations or on appeal, we will use the abbreviation "ECJ" (standing for the "[**E**uropean] **C**ourt of **J**ustice"). If a judgment is handed down by the **G**eneral **C**ourt (formerly the Court of First Instance – "CFI"), we will use the abbreviation "GC".

following documents for parties' representatives:
- Aide-mémoire – Application;
- Model summary of the pleas in law and main arguments relied on in the application;
- Aide-mémoire – Hearing of oral argument;
- Omission of data vis-à-vis the public in judicial proceedings. (CR)

CJEU's 2022 Judicial Stats

According to its judicial statistics for the year 2022, the CJEU confirms a structural increase in the number of cases brought before the Court of Justice and the General Court of the European Union. As in previous years, both courts together received more than 1500 cases.

The key statistics for both courts:
- In 2022, the Court of Justice received 806 new cases, the General Court 904 new cases;
- Both courts completed 1666 cases;
- 2585 cases were pending before both courts.

The key statistics for the Court of Justice:
- The average duration of preliminary ruling proceedings before the court increased slightly from 16.7 months in 2021 to 17.3 months in 2022;
- The court noted an increased number of cases with sensitive and complex issues, calling for greater reflection and time;
- References for a preliminary ruling came mainly from German (98), Italian (63), Bulgarian (43), Spanish (41), and Polish (39) courts.

The key statistics for the General Court:
- The year 2022 was marked by the emergence of cases involving the restrictive measures adopted by the EU in the context of the war in Ukraine;
- Cases involving restrictive measures represented 11.4% of all new cases brought before the court in 2022;
- The average duration of proceedings closed by judgment or by order was 16.2 months (compared to 17.3 months in 2021) and 20.4 months for cases closed by judgment only.

To preserve its capacity to deliver high-quality decisions within a reasonable time, the Court of Justice submitted on 30 November 2022 a request to the EU legislature with a view to amending Protocol No 3 on the Statute of the Court of Justice of the EU. In concrete terms, the Court of Justice is seeking a transfer of jurisdiction to the General Court to give preliminary rulings in certain specific areas:
- The common system of value added tax;
- Excise duties;
- The Customs Code and the tariff classification of goods under the Combined Nomenclature;
- Compensation and assistance to passengers;
- The scheme for greenhouse gas emission allowance trading.

It is also seeking an extension of the mechanism to determine whether an appeal can be allowed to proceed against decisions of the General Court. (CR)

New Registrar at the General Court

On 26 April 2023, Mr *Vittorio Di Bucci* was appointed Registrar of the General Court of the EU. Prior to his appointment, Mr Di Bucci, who joined the European institution in 1987, served as principal legal adviser/director in the Legal Service of the European Commission, heading the business law team. Di Bucci succeeds Mr *Hans Jung* (1989–2005) and Mr *Emmanuel Coulon* (2005–2023). (CR)

OLAF

New Working Arrangement Fosters Cooperation between Eurojust and OLAF

On 29 March 2023, Eurojust and OLAF signed a new Working Arrangement to enhance their cooperation in the fight against fraud, corruption, environmental crime, intellectual property crime, and other crimes affecting the EU's financial interests. The Working Arrangement replaces the 15-year-old Practical Agreement on arrangements of cooperation between Eurojust and OLAF signed in 2008.

The new Working Arrangement outlines practical details of the institutional, strategic, and operational cooperation between Eurojust and OLAF. Both parties will establish liaison teams to serve as contact points and coordinate cooperation between the two agencies and to prepare the annual high-level meetings between OLAF's Director-General and Eurojust's President. OLAF and Eurojust agree to exchange information of a strategic nature and collaborate with regard to training, workshops, seminars, and conferences. The secondment of a representative to the other party is also possible.

In the area of operational cooperation, the bodies may, for instance, provide each other with mutual assistance and advice, seek judicial recommendations, and participate in coordination meetings, coordination centres, and other operational meetings. Furthermore, they may cooperate in Joint Investigations Teams (JITs) by informing the other party of a relevant JIT and asking the relevant Member State to invite the other party to take part in it. In addition, OLAF may request Eurojust to ask the competent authority of the Member States concerned to set up a JIT in cases dealing with an illegal activity within OLAF's mandate. Lastly, the Arrangement sets out detailed rules for the exchange of operational information, respective communication channels, data protection rules, access to documents, communication with the media, and expenses. The new Working Arrangement had immediate effect and entered into force on 30 March 2023. (CR)

OLAF Fosters Cooperation with State Audit Service of Ukraine

On 27 March 2023, OLAF Director-General *Ville Itälä* signed an administrative cooperation arrangement with the State Audit Service of Ukraine (SAS). The SAS is the national contact point for cooperation with OLAF. The arrangement will facilitate the exchange of information and cooperation in investigative activities.

OLAF will also support the Ukrainian authorities in their national anti-fraud efforts and strategies, for example by helping increase anti-fraud knowledge for prevention, by contributing to capacity building and by providing training to protect EU funds. It is also envisaged that Ukraine is associated to the Union Anti-Fraud Programme (UAFP).

Cooperation with Ukrainian authorities is important since the EU has delivered unprecedented financial support after Russia's aggression, and will continue to do so in the future. The fight against corruption and fraud will therefore be key to protect the taxpayers' money and to help Ukraine emerge from war damage. (TW)

OLAF Gets Access to Spanish Notaries' Data

On 22 March 2023, OLAF signed a cooperation agreement with the General Council of Notaries of Spain (CGN). The core feature of the agreement is that OLAF will be enabled to have access to the data of the CGN's Centralized Body for the Prevention of Money Laundering (OCP).

The databases include data on beneficial owners of over 2.4 million commercial entities, nearly 164,000 non-commercial legal entities, such as associations, foundations or political parties, and more than 50,000 foreign entities. In addition, another database identifies nearly 25,000 persons who hold public responsibility by election or designation; nearly 31,000 related persons (family members and persons with professional or commercial ties) and over 4,000 companies in which persons with public responsibility hold shares (data from January 2021).

The Single Computerised Notarial Index stores and electronically classifies the content of the deeds and public acts authorised by the more than 2,800 Spanish notaries leading to a bulk of information on public documents.

Access to these data sources is considered extremely helpful for OLAF since perpetrators of EU fraud often hide their traces behind intricate schemes of companies and corporate entities. The CGN will set up a web platform from which OLAF's information requests will be channelled. (TW)

OLAF Signs Arrangements with US Authorities

On 20 March 2023, OLAF Director-General *Ville Itälä* signed two administrative cooperation arrangements with partners in the USA.

The arrangement with the U.S. Bureau of Industry and Security sets out the framework for cooperation in the fight against customs fraud, in particular regarding trade in prohibited or restricted goods. It will facilitate the exchange of strategic information and risk analysis and foster assistance in investigations.

The arrangement with the U.S. International Development Financing Cooperation (DFC) covers the prevention of double financing and the possibility of joint or parallel investigations, technical assistance and strategic analysis. Cooperation enables OLAF better oversight in multiple countries where the DFC is active.

By the new arrangements, OLAF expands formal partnerships with US authorities. Administrative cooperation arrangements already exist with the United States Agency for International Development (USAID) and the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives. (TW)

Illicit Tobacco Trade in 2022

On 4 April 2023, OLAF presented the results of its operations against tobacco smuggling in 2022. For the results in 2021 →eucrim 1/2022, 14; for the results in 2020 →eucrim 1/2021, 14.

International operations involving OLAF throughout 2022 led to the seizure of 531 million contraband cigarettes, more than 205 tonnes of raw tobacco, and 65 tonnes of water-pipe tobacco. Investigations indicated that there is an increasing trend towards illicit factories combining raw materials in the European Union. Nearly 60% of the cigarettes seized (over 316 million cigarettes) had been illegally produced in the EU. In addition, around 200 million cigarettes could be prevented from entering the EU at its external borders. 2022 also saw an increase in the smuggling of water-pipe tobacco, another emerging trend.

Smuggling networks usually take advantage of the differences and gaps between the various national systems. OLAF's role is, above all, to gather intelligence, to put the relevant information together and into concrete operations, and to promptly provide the competent national authorities with this information, so that they can take action. (TW)

OLAF's Operational Work: January–May 2023

This news item summarises OLAF's operational work from January to May 2023 in chronological order:

- 23 February 2023: OLAF concludes investigations into a project in Hungary which was designed to equip elementary and high schools with digital technologies. The project was funded by the European Social Fund. OLAF detected several breaches in public procurement procedures and recommends that the competent Commission directorate recovers more than 3.6 million.
- 29 March 2023: OLAF is awarded the Montreal Protocol Award for Customs and Enforcement Officers for

its work against smuggling in ozone-depleting substances and fluorinated global warming substances controlled under the Montreal Protocol. Tackling illicit trade in climate-damaging gases has been one of OLAF's operational priorities for several years. OLAF's operations led to the seizure and detention of almost 800 tonnes of illegal refrigerants over the past few years.

- 31 March 2023: OLAF reports that it supported the successful seizure of 11 tonnes of pesticides in a joint action with the Bulgarian Food Safety Agency and the Bulgarian National Police General Directorate. Investigators found several violations, including the trade with banned substances in the EU. OLAF stressed that several illicit substances seized are very dangerous for human health and bees.
- 10 May 2023: In a joint action, French and Spanish authorities with the support of OLAF, Europol, and Eurojust were able to dismantle an organised crime group that illegally breeded and trafficked eels. 1.5 tonnes of live eels were seized, 27 persons arrested and financial assets valued at €2 million frozen. (TW)

European Public Prosecutor's Office

ECBA: Courts in the Assisting Member State Must Have Full Review Powers

On 27 February 2023, the ECJ held a Grand Chamber hearing in the first reference for a preliminary ruling dealing with the interpretation of the EPPO Regulation (Case C-281/22, *GK and Others* →eucrim 2/2022, 96). On the eve of this hearing, the European Criminal Bar Association (ECBA) published an open letter in which the views of the defence lawyers on the case are presented. The reference for preliminary ruling by the Oberlandesgericht Wien concerns the question as to which extent the courts of the assisting European Delegated Prosecutor (EDP) can verify an investigative measure under their national law when it was authorised in the Member State of the EDP handling the case (→analysis by *A. Venegoni,* eucrim 4/2022, 282).

First, the ECBA points out the existing structural inequality of arms in EPPO proceedings: while the EPPO as an institution is allowed to participate actively in the proceedings before the CJEU, defence lawyer organisations representing the bars cannot intervene.

Second, the ECBA strongly advocates that the courts in the assisting EDP's Member States must be allowed to review the substantive reasons for the investigative measure to be adopted. A substantive review by the courts in the assisting Member State is already required in order to assess fundamental rights, immunities and privileges (such as legal privilege) that exist in the laws of the assisting Member State. The ECBA further argues that legal reviews in the assisting Member State cannot be a mere rubber-stamping exercise when it comes to mutual legal assistance situations under the EPPO regime.

Third, the ECBA opposes the argument that legal reviews in cross-border cooperation situations under the EPPO regime cannot be more cumbersome than in the system established by the European Investigation Order (EIO). According to the ECBA, the courts in the Member States executing an EIO would also have the power to review the "substantive reasons" for issuing a measure if the fundamental rights of persons targeted by investigative measures are at stake.

In sum, the ECBA's open letter emphasises that an interpretation of the EPPO Regulation in Case C-281/22 should not lead to a preponderance of the effectiveness of EPPO investigations. (TW)

Jean Monnet Module on the European Public Prosecutor's Office at Milano-Bicocca University: Promoting European Integration through the EPPO

The Jean Monnet Module "EPPO and EU Law: A Step Forward in Integration" (STEPPO) hosted by Milano-Bicocca University is a 3-year teaching module, which offers insights into the functioning of the European Public Prosecutor's Office (EPPO). The project began in 2021; it is co-funded by the EU Erasmus+ Programme (European Commission) and supported by the European Parliament.

The Module's participants can learn more about the EPPO through dialogue between prosecutors, law enforcement officers, EU officials, customs authorities, legal practitioners, academics, students, and the general public. Key achievements of the module include:

- Dissemination of learning modules (290 attendees in 2023);
- Leveraging social media with more than 70 blogs and posts that have been published on the website (>1000 users involved);
- A digital collection of lessons on the website with direct and open access to video recordings and presentations of the sessions using VR Code technology;
- Development of VR training (in progress) to enable attendees to participate in an EPPO investigation simulation;
- Database of cases, containing (so far) over 50 cases from various EU Member States on the topic;
- A strong network of professionals from different legal spheres is organised in the form of 19 subcommittees of the Module.

Moreover, after the expiration of the Module, the project group will continue its work in the form of the Jean Monnet Centre of Excellence starting in 2024 (EPPO: A New Frontier in Integration (EPPONFI)). This Centre of Excellence has been officially supported by the European Commission and will last until 2026.

More information on the STEPPO and upcoming EPPONFI is available at: <https://www.steppo-eulaw.com/>.

Ass. Prof. Benedetta Ubertazzi (Module Coordinator) and Antony Zhilkin, Milan-Bicocca University

EPPO's Annual Report for 2022

On 1 March 2023, the EPPO presented its annual report for 2022. It is the first annual report that provides the picture of a full calendar year after the EPPO had started to exercise its competence on 1 June 2021 (for the first annual report covering the period of operations from 1 June to 31 December 2022 →eucrim 1/2022, 15–16). In 13 chapters, the annual report for 2022 provides information, *inter alia*, on the following issues:

- EPPO's operational activity, including figures from each participating Member State;
- The activity of EPPO's organisational entities, such as the College, the Permanent Chambers, the European Delegated Prosecutors, and the Operations and College Support Unit;
- The Case Management System and IT;
- Human resources and staff development;
- Relations of the EPPO with its partners, including relations with non-participating Member States and third countries.

The EPPO reports that it processed 3318 crime reports and opened 865 investigations in 2022. Judges granted the freezing of €359.1 million in EPPO investigations, more than seven times the body's 2022 budget. Other key figures include the following:

- By the end of 2022, the EPPO had a total of 1117 active investigations for overall estimated damages of €14.1 billion;
- Over 28% of the active investigations had a cross-border dimension;
- The EPPO opened 865 investigations with estimated damages of €9.9 billion;
- Regarding the typologies identified in the active cases, most (679) deal with non-procurement expenditure fraud followed by VAT fraud (427 cases);
- Nearly half of the estimated damages (€6.7 billion) concerns VAT fraud;
- The proportion of reports about suspicions of fraud from private parties is at 58%;
- 114 European Delegated Prosecutors in active employment;
- 217 staff members at the central office in Luxembourg.

When presenting the report, European Chief Prosecutor *Laura Kövesi* stressed that, in 2022, the EPPO demonstrated its unprecedented capacity to identify and trace volatile financial flows and opaque legal arrangements. She added that the EPPO, however, is far from having reached its full potential. In doing so, the EPPO Regulation should be reviewed as soon as possible on several critical aspects. (TW)

Arrangement between EPPO and Hellenic Independent Authority of Public Revenues Signed

On 17 February 2023, the EPPO signed a working arrangement with the Hellenic Independent Authority of Public Revenues (IAPR). The arrangement aims to provide a structured framework for closer cooperation, in particular through the following:

- Establishing modalities and channels for the exchange of information;
- Ensuring that the IAPR provides the EPPO with the appropriate investigative support;
- Ensuring that the IAPR conducts investigations in EPPO cases as a matter of priority;
- Setting out further possibilities of customized cooperation, including the exchange of strategic information.

According to the arrangement, the IAPR will identify and inform the EPPO of all cases that fall within EPPO's mandate. In the course of EPPO investigations, the IAPR will provide support by giving access to information and databases, supplying technical expertise, and undertaking preliminary investigations.

The arrangement also foresees that both parties designate contact points for operational cooperation. The EPPO and the IAPR will organise regular high-level meetings as well as technical meetings at both operational and administrative levels.

Given the IAPR's key role in the Greek system, the arrangement will strengthen the fight against organised crime connected to smuggling of goods, corruption, fraud, including cross-border VAT fraud, and any other criminal offence or illegal activity adversely affecting the European Union's financial interests. (TW)

Convictions in VAT Carousel Fraud Case with Luxury Cars

German criminal courts handed down first judgments in a major EPPO case that dismantled a VAT carousel fraud ring involving luxury cars. This scheme was investigated since 2021 by the EPPO in Germany, and is estimated to have caused losses of at least €13 million (→eucrim 4/2021, 211). In an operation in October 2021, ten suspects were arrested and afterwards indicted. It was revealed that three suspects have links to the Italian mafia organisation ‚Ndrangheta. Thanks to EPPO's investigations, law enforcement authorities also prosecuted suspects for major drug trafficking offences involving Germany, Italy and Bulgaria.

On 16 December 2022, the Regional Court of Ingolstadt (Germany), handed down the first judgment against one of the arrested persons. The defendant was given a combined sentence of nine years' imprisonment for tax evasion and drug trafficking with weapons.

On 13 February 2023, the Regional Court of München II convicted four more suspects. Having found them guilty for VAT fraud, three suspects will have to serve prison sentences of between 2 years 3 months and 3 years, and the fourth received 1 year and 10 months of probation. Moreover, the court made a confiscation order of over €1 million.

On 28 March 2023, the Regional Court of Landshut imposed sentences

on two other defendants for VAT fraud. They will have to serve prison sentences of 4 years and 9 months, and 2 years and 9 months, respectively. In addition, the court made a confiscation order of over €5 million. (TW)

Overview of Convictions in EPPO Cases: January–April 2023

The following provides an overview of court verdicts in EPPO cases in the various participating EU Member States, as far as reported by the EPPO. It covers the period from 1 January to 30 April 2023 and continues the overview in eucrim 2/2022, 96. The overview is in reverse chronological order.

■ 11 April 2023: The EPPO in Bratislava (Slovakia) files an appeal against the judgement of the Specialised Criminal Court in Slovakia in a VAT fraud case based on the overevaluation of machinery to obtain EU funds. The EPPO seeks verification of the light sentences against the two main offenders (seven years' imprisonment and five years and six months' imprisonment, respectively) and an acquittal of another defendant. In addition, the EPPO questions the legal qualification which should consider that the crimes were committed by an organised group.

■ 5 April 2023: After the EPPO had filed an indictment on 10 March 2023, the Zemgale District Court in Riga (Latvia) convicts two individuals for fraud involving EU agricultural funds. The first defendant was given a suspended sentence of two years and nine months' imprisonment, the second defendant was given a suspended sentence of two years and six months' imprisonment. In addition, both individuals must pay a fine and are excluded from applying to EU-funded projects until 2025. €100,000 of unlawfully obtained EU funds were fully recovered before the trial. The sentence is based on plea bargains between the defendants and the EDP.

■ 4 April 2023: In the context of a large-scale VAT fraud case conducted by the EPPO in Milan, a police officer of the Guardia di Finanza is sentenced to five years of imprisonment for corruption. The Tribunal of Brescia found that the official received bribes of €50,000 from a businessperson, with the purpose of softening or excluding the businessperson's responsibilities, and those of some of his family members, from the criminal investigation in the VAT case. The Tribunal also ordered the confiscation of €50,000 as proceeds of the crime, and the extended confiscation of additional property – believed to derive from criminal conduct – with a value of over €470,000.

■ 16 February 2023: The Paris Criminal Court passes the first verdict of an EPPO case in France. The director of a rental car company was given an 18-month conditional sentence. His accomplice was sentenced to five months' imprisonment, that was also suspended. In addition, the convicted persons were sentenced to jointly pay a fine of €150,000. The defendants imported luxury cars from Switzerland to France without paying customs duties and import VAT; damages of €110,000 incurred to the EU and the national budgets. The case before the Paris criminal court was concluded by a simplified procedure in which the defendants pleaded guilty to all charges. The director was ordered to pay the damages to the EU and the national treasury in full.

■ 15 February 2023: The Regional Court of Frankfurt (*Landgericht Frankfurt*) convicts two persons for VAT fraud. The first defendant was sentenced to five years and nine months of imprisonment. He was the head behind a VAT carousel fraud scheme that illegally received more than €33 million for businesses with Voice over Internet Protocol (VoIP) services. He handled several fake companies and issued false invoices for VoIP services that never took place. The second defendant was given a suspended sentence of two years. He knew the fraudulent activities and did not ensure proper taxation. The case involved several tax investigation offices in Germany. (TW)

EPPO's Operational Activities: January–April 2023

The following provides an overview of EPPO's main operational activities in the first four months of 2023 (1 January – 30 April 2023). It continues the periodic reports of the last issues (for the previous overview →eucrim 4/2022, 236–237). The overview is in reverse chronological order.

■ 21 April 2023: Investigations by the EPPO in Palermo (Italy) lead to house arrests of three suspects. A public school principal and her deputy are suspected of having embezzled EU and national funds for school projects in disadvantaged communities. School projects had not or partially not been implemented, and expensive computers, which were intended for the pupils, were stored inside the principal's office where they were misappropriated by the principal and her deputy. In addition, the third suspect's company was seemingly unlawfully favoured to supply the technological material following the payment of bribes. Damages to the budgets are estimated at over €100,000.

■ 4 April 2023: In the context of a probe into a tobacco fraud scheme led by the EPPO in Iași (Romania), Romanian law enforcement authorities seize real estate and cash in different currencies in order to recover damages to the national and EU budgets. Under suspicion are several individuals (including customs officials) and companies from Czechia, Germany, Italy, Lithuania, Poland, Slovakia and Ukraine. They allegedly built up a system of disguising movements of tobacco products imported from the United Arab Emirates and Turkey. Shipments of processed tobacco products were declared as being in transit through the

EU with destinations to non-EU countries (for which excise duties and VAT is suspended), but instead the goods were sold within EU countries at huge profits. The losses amount at least to €650,000.

■ 4 April 2023: The EPPO has five individuals arrested in Croatia. Together with a company, they are suspected of having committed criminal offences of abuse of office and authority, in connection with the public procurement proceedings for the project of construction of a plant for sorting collected waste, located at Mihačeva Draga (Croatia).

■ 31 March 2023: The Bulgarian police is looking for the seizure of documents and electronic evidence in several locations in Sofia (Bulgaria). The underlying EPPO investigation deals with corruption and the mismanagement of funds that had been allocated to the restoration of Sofia's historic centre. It is believed that undue payments were made because contractors falsely certified that works had been carried out in accordance with specifications. The works were co-financed by the European Regional Development Fund (ERDF). Following media reports, the EPPO opened investigations "*ex officio*" in autumn 2022. The estimated damage is at least €3 million.

■ 28 March 2023: The Belgian police carries out a raid in several locations in Belgium, including at Liège Airport, and arrests four suspects. The code-named operation "Silk Road" is led by the EPPO in Brussels and supported by Europol and other Belgian customs, tax and law enforcement authorities. The investigations target Chinese exporters who built up a complex system that allowed the evasion of VAT and customs duties for their exported goods (electronic equipment, toys and accessories). The suspects disguised that the goods have not been further transported to other EU Member States after importation (for which VAT is exempted). Instead, the goods were directly sold to consumers with prices including VAT which has never been paid to the tax authorities. In order to evade payments of VAT and customs duties, criminals used private customs authorities that falsely declared the final destination, established shell companies in various EU Member States, and submitted false invoices and falsified transport documents. It is believed that the damage to the budgets is around €310 million.

■ 23 March 2023: An EPPO investigation involving the EU Next Generation Programme revealed an alleged fraud up to €1 million by an Italian company and its representative. The legal representative is put under house arrest. He is suspected of having submitted several falsified applications for subsidised loans and non-repayable funds.

■ 23 March 2023: The EPPO in Bologna (Italy) has assets worth up to €149 million seized. EPPO investigations target a Missing Trader Intra-Community (MTIC) fraud with fuels. Three Italians are suspected of having formed a criminal group by introducing fuel products into the Italian territory from other EU Member States for their subsequent resale at a low cost, using a string of shell companies and a buffer company. It is estimated that more than €92 million VAT have been unpaid since the existence of the scheme in 2016.

■ 21 March 2023: In an operation led by the EPPO in Naples and Milan (Italy), the Guardia di Finanza arrests 12 persons (five entrepreneurs, three accountants and four public officials). They are suspected of being part of a professional organised crime group located in Naples that sold VAT evasion schemes. The case involves a complex VAT carousel with over 170 shell companies in several European countries and the USA. In order to evade VAT payments, fictious invoices were issued for the trade in electronic equipment (mainly AirPods). In addition to the arrests, a freezing order for a value of approximately €8 million was executed.

■ 9 March 2023: Upon request by the EPPO, Romanian law enforcement authorities carry out house searches in five counties in Romania and arrest three suspects. The suspects are accused of having collaborated in unduly receiving money from the European Structural and Investments Funds. They provided false documents and inflated equipment costs and thus received EU money for their personal profits.

■ 9 March 2023: The EU-funded event "Water – World Forum for Life" that took place in Reguengos de Monsaraz (Portugal) in June 2021 to raise awareness of environmental sustainability is subject to EPPO investigations. The Portuguese Polícia Judiciária carries out searches in the municipality for suspicion of subsidy fraud, active and passive corruption and financial complicity in business fraud by a public official. The fraud may concern over €800,000.

■ 6 March 2023: In a case involving the supply of protective masks during the COVID-19 pandemic in Spain, EPPO's Permanent Chamber dismisses the criminal proceedings. It was found that the price paid for the masks was not disproportionate in relation to the quality of the material offered and delivered. It seemed that the public money (the contract was worth more than €1.5 million for 250,000 FFP2–3 masks) was spent correctly.

■ 3 March 2023: The Guardia di Finanza executes a preventive seizure order against a farmer in Sicily. In an EPPO investigation, the farmer is suspected of having made false statements and submitted false lease contracts in order to receive money from the EU agricultural funds. The farmer claimed to be in possession of parcels of land which he has actually never owned. The damage to the EU budget is estimated at around €600,000.

■ 27 February 2023: Bulgarian law enforcement authorities carry out seizures and other investigative measures in the context of EPPO investigations into multi-million euro fraud regarding greenhouse gas emissions. A private Bulgarian company is suspected of having knowingly submitted false data in annual reports on greenhouse gas emissions produced by thermal power plants and heating plants in Bulgaria. Thus, competent national authorities were misled as to the actual amount of emissions and these remained unpaid under the EU Emissions Trading System (EU ETS). Losses for the EU and national budgets ran into millions.

■ 23 February 2023: In EPPO investigations against MEP *Stefania Zambelli* and four of her assistants, the Guardia di Finanza in Brescia seizes bank accounts and luxury cars worth more than €170,000. This is the damage allegedly caused by MEP *Zambelli* and her staff members to the EU budget because of false declarations of the work assistants were hired for and for having declared false educational and professional skills. According to the investigations, the assistants have not or only partially carried out activities for the European Parliament despite of having received parliamentary allowances.

■ 22 February 2023: It is revealed that operation "VAT Games" (see below) has connections with a VAT carousel fraud investigated by the EPPO in Madrid (Spain). In operation "Marengo Rosso", law enforcement authorities in Spain, Czechia, Hungary, Italy, Luxembourg, Portugal, Poland, and Slovakia crack down on a criminal organisation that is believed to have orchestrated a massive €25 million VAT fraud through the sales of mobile phones and other electronic equipment. The ringleader is supposed to have been arrested on 17 February in Milan under operation "VAT Games" following another investigation by the EPPO in Milan. Operation "Marengo Rosso" led to the arrest of 17 persons and the seizure of a considerable amount of assets, including real estate and luxury cars. The arrested persons are alleged to have established a chain of shell companies by which they received unjustified VAT reimbursements for the trade in electronic devices and equipment. Illicit profits were laundered and reinvested in high-value real estate in different countries. Europol and Eurojust were also involved in the law enforcement action against the criminal organisation.

■ 17 February 2023: Six persons are arrested and assets are seized in a major operation led by the EPPO in Milan (Italy). The operation dubbed "VAT Games" targeted a criminal organisation that established a complex network of companies in order to commit VAT carousel fraud. Companies were established in Bulgaria, the Netherlands, Poland and Slovakia from where they sold electronics and computer equipment to shell companies in Italy. The latter ones were administered by figureheads, in order to evade the payment of VAT. The estimated VAT losses are around €40 million. First actions against the organisation were already carried out in October 2022.

■ 15 February 2023: On the EPPO's request, law enforcement authorities take action against an organised criminal group in Iaşi (Romania). 13 houses and premises are searched. 12 individuals are confronted with findings that they have fraudulently obtained €1.6 million from employment funds. The EU co-financed trainings of unemployed people. It was revealed, however, that employment contracts were only formally terminated in order to receive the money and some trainings never happened. The suspects provided false documents and certificates.

■ 9 February 2023: In an investigation code-named "Water Diviner" the EPPO has €1.6 million seized in Italy. The investigations involve an Italian start-up that promised to develop "thermodynamic machines" for the purification and filtering of water in remote areas and thus received money from EU and regional funds. However, the machines have never gone operational. The start-up falsified statements and certificates, provided fraudulent assurances and rigged tenders. The case was initially opened by OLAF in 2020 and later taken over by the EPPO.

■ 1 February 2023: In an EPPO-led operation, Italian and French law enforcement authorities crack down on several suspects of an organised criminal group that smuggled counterfeited cigarettes from Tunisia to Italy before selling them on the Italian and French black markets. Investigations against the group were already opened by the Public Prosecutor's Office of Genoa (Italy) in September 2020 and the case was taken over by the EPPO in December 2021. The damage to the public budget is at least €450.000.

■ 31 January 2023: The EPPO in Vilnius (Lithuania) indicts six defendants for fraud relating to procurement procedures, which caused damages of €580 000 to the EU budget. The defendants colluded in manipulating tenders and issuing fictious invoices. The defendants confessed to having committed the criminal offences and the damage to the EU budget could be fully recovered.

■ 31 January 2023: The Guardia di Finanza in Palermo carries out a preventive seizure order of over €7 million, requested by the EPPO in Palermo. The suspects are believed to have fraudulently received agricultural funds by issuing invoices with a higher price than the actual price of their expenses.

■ 26 January 2023: The EPPO and the Guardia di Finanza in South Tyrol crack down on an organised criminal group that built up a VAT evasion scheme on the trade in stationery and consumables for printing equipment. The operation, code-named "Cheap Ink", led to the arrest of 18 suspects and the seizure of money and financial assets, vehicles and real estate of a total val-

ue of approximately €58 million. The EPPO in Italy cooperated with investigators from Czechia, Poland, Austria, Slovakia, the Netherlands, Germany and the UK.

- 24 January 2023: The EPPO carries out an action day for an investigation led by the EPPO in Munich. 61 business premises are searched and 5 persons arrested. "Operation Display" involves 10 EU countries and targets a organised criminal group that established a missing trader intra-community fraud scheme for the trade in small electronic devices in Europe. The EPPO in Munich began investigations short after the start of EPPO's operations in June 2021. The estimated loss of VAT is around €32 million.
- 24 January 2023: The EPPO in Riga has searches carried out and persons arrested at Daugavpils University (Latvia). Suspects are believed to have illegally received €600,000 from the European Social Fund by rigging public procurement procedures.
- 23 January 2023: The EPPO in Zagreb (Croatia) indicts six defendants for the criminal offences of illegal trade of cigarettes, tax or customs duty evasion and bribery. They were allegedly part of a criminal organisation that smuggled cigarettes from Dubai to Croatia without paying taxes. The damage to the public finances is estimated at around €3.3 million.
- 17 January 2023: The Guardia di Finanza executes search, seizure and freezing orders (requested by the EPPO) against a company located in Lecco-Brianza (Italy). Italian managers of the company constructed a tax evasion scheme with bogus companies in the Netherlands achieving exempt of VAT from their products actually merchandised in Italy. The registration of several ostensible companies in the Netherlands, including in tax havens such as the Netherlands Antilles, for tax evasion purposes is also knows as the "Dutch sandwich". It is estimated that VAT of over €10 million has not been paid between 2013 and 2018.
- 11 January 2023: The EPPO in Hamburg (Germany) updates on the investigations against an international criminal group that operated also in Lithuania, the Netherlands, and Estonia and that deceived customs authorities as to the true value of imported luxury cars (→eucrim 1/2022, 17–18). €3.5 million were lost in import duties. The EPPO seized several smuggled luxury cars for a total value of almost €1 million and brought 32 cases to trial before the Osnabrück Regional Court (*Große Wirtschaftsstrafkammer, Landgericht Osnabrück*).
- 5 January 2023: The EPPO starts an investigation into EU subsidy fraud against an individual and a company in Zlín (Czechia). They are suspected of having submitted false invoices in order to receive more money from the EU Structural Fund that financed the expansion of a technological centre. Update: In June 2023, the EPPO revealed the involvement of two more individuals and two more companies suspected of having helped the main suspect to receive €1.8 million in EU funds. (TW)

Europol

Agreement between Europol and New Zealand Approved

On 14 February 2023, the Council of the EU approved an Agreement between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement (Europol) and the authorities in New Zealand competent for fighting serious crime and terrorism. The agreement enables the transfer of personal data between Europol and the competent authorities in New Zealand, with a view to fighting serious crime and terrorism and protecting the security of the Union and its inhabitants. It includes provisions on the exchange of information and data protection, the rights of data subjects, the establishment of a supervisory authority, and administrative and judicial redress.

The agreement was formally published in the EU's Official Journal on 20 February 2023. It enters into force on the date of receipt of the last written notification in which the contracting parties notify each other that the respective procedures have been completed through diplomatic channels.

The agreement will be one of the first ones under the current Europol's legal framework, i.e. Regulation 2016/794, which provides that it is possible for Europol to transfer personal data to an authority of a third country on the basis of a bilateral agreement between the EU and the third country. Currently, Europol works together with the New Zealand Police on the basis of Working Arrangement concluded in 2019. The Arrangement has not provided a legal basis for the transfer of personal data by Europol to the law enforcement authorities of New Zealand.

The concluded Agreement will allow the exchange of personal data for the first time that is linked to serious crime and/or terrorism. It had been mainly motivated by the terrorist attacks in Christchurch in March 2019. (CR)

Europol Enhances Cooperation with ICC

On 25 April 2023, Europol and the International Criminal Court (ICC) signed a Working Arrangement to enhance their cooperation, in particular through the exchange of information, knowledge, experience, and expertise inherent to their respective mandates. Areas of cooperation under the Arrangement include the following:

- Exchanging specialist knowledge;
- Evidence gathering;
- Generating general situation reports;
- Sharing results of strategic analysis;

- Exchanging information on criminal investigation procedures;
- Providing information on crime prevention methods;
- Participating in training activities;
- Providing advice and support in individual criminal investigations.

Both parties shall designate points of contact and organise regular high-level meetings. The ICC may agree to deploy Liaison Officers to Europol. The establishment and operation of a secure communication line for the purpose of exchange of information between Europol and the ICC is also envisaged. Furthermore, the Arrangement sets out rules for the onward transmission of information, the exchange of personal data, the security of information, and for disputes and liability. (CR)

Successful EU Most Wanted Fugitives Campaign 2022

With 14 cases of fugitive criminals solved, the 2022 campaign of the Europe's Most Wanted Fugitives website marked its most successful year since 2019. The website, launched in 2016, provides profiles of fugitives and the possibility to send a (anonymous) message to the ENFAST teams to help find them. Since the website's start, 392 profiles of fugitives have been listed and 136 of them have been arrested, with 49 of those arrests being directly linked to publication of the fugitive profile on the website. The European Network of Fugitive Active Search Teams (ENFAST) used social media and billboards in Brussels and Barcelona to increase public awareness of the campaign. A far-reaching communication campaign by Europol also helped make the 2022 campaign so successful. (CR)

Europol Organised First Forensic Sprint

For the first time, Europol organised a "Forensic Sprint" at its headquarters. 15 experts from eight countries met at Europol HQ from 6 to 9 March 2023 in order to jointly extract data from seized devices. The sprint built on previous raids that had been conducted against a Chinese sexual exploitation ring within the Operational Task Force Lotus. During the raids in February of this year, 31 suspects were arrested (for their alleged involvement in the sexual exploitation of Chinese victims), 200 victims identified, and hundreds of mobile devices seized. The devices were being used by the suspects to communicate with clients and send instructions to the victims. By means of the forensic sprint, data from these devices were able to be extracted much more quickly and efficiently than if each country had performed this task itself. (CR)

Eurojust

New Administrative Director at Eurojust Takes Office

1 March 2023 marked the beginning of the mandate of Eurojust's new Administrative Director, Mr *Evert van Walsum*. For the next four years, Mr van Walsum, a Dutch national with long-standing experience in managerial positions for national and European financial regulators, will be responsible for the day-to-day administration and staff management of Eurojust (→eucrim news of 23 November 2022). (CR)

New National Member for Estonia at Eurojust

At the beginning of March 2023, Ms *Piret Paukštys* took up her five-year mandate at Eurojust as new National Member for Estonia. Prior to joining the EU's Agency for criminal justice cooperation, Ms Paukštys worked as state prosecutor in the Estonian Office of the Prosecutor General, where she specialised in the prosecution of economic, financial, and cybercrime cases as well as in international cooperation matters. Ms Paukštys succeeds Ms *Laura Vaik*. (CR)

New National Member for Bulgaria at Eurojust

In May 2023, Ms *Biserca Ivanova Stoyanova* commenced her five-year mandate as National Member for Bulgaria at Eurojust. Prior to joining Eurojust, Stoyanova worked for several Bulgarian investigation services as an investigating magistrate for over 26 years. Her last position was as Head of First Specialised Department at the National Investigation Service in Bulgaria. Ms Stoyanova succeeds Ms *Ivanka Kotorova*. (CR)

European Judicial Network (EJN)

EJN Provides Form for MLA with UK

In order to assist with requests for mutual legal assistance in criminal matters to the UK under the Trade and Cooperation Agreement, the EJN now offers a form that can be downloaded from its website. The form, which can be used on a voluntary basis, is available in all EU languages in Word format. Information about the UK's competent authorities and other important practicalities can be found by referring to the UK section of the EJN website. The EJN plans to integrate the forms into its Compendium which facilitates the drafting of requests for MLA. (CR)

EJN Launched Updated E-tools

On 9 February 2023, the EJN launched its improved, more user-friendly e-tools Atlas, Fiches Belges, and Compendium. The tools are tailored to assist practitioners in drafting and sending requests for mutual legal assistance. They are publicly available on the EJN website without prior authorisation for use.

- Atlas helps practitioners find the competent authority in the EU Member States and Norway for communicating a request, depending on the required investigative/procedural measure;

- Fiches Belges contain concise and practical information on the national regulation of investigative/procedural measures such as, for instance, the European Arrest Warrant or the European Investigation Order;
- Compendium is intended to facilitate the drafting of a request directly via the EJN website, automatically completing those parts of the form that require the population of the details of the relevant competent authorities. The forms can also be printed and sent. (CR)

Frontex

Frontex Annual Report 2022

On 28 February 2023, Frontex published its Annual Report for the year 2022. The report outlines the changes Frontex saw in 2022, gives a picture of the deployment of its standing corps and their operational support, and provides examples of its crisis response. It illustrates the agency's fight against cross-border crime, its work regarding return and reintegration, and its efforts to put fundamental rights at the centre of its activities.

In 2022, Frontex deployed more than 2000 standing corps officers at the EU's external borders every month. Outside the EU, the agency was active in operations in Moldova, Serbia, Montenegro and Albania. A crisis response team/mechanism provided support at the EU-Ukraine borders and assisted non-Ukrainian and non-EU citizens fleeing the war in Ukraine in reaching their home countries. Five joint action days were also coordinated by Frontex to deal with drug and firearms smuggling, document fraud, stolen cars, and the trafficking of human beings (THB).

Other noteworthy figures are: In 2022, 24,850 persons were returned and 53,000 persons were rescued at sea with Frontex' support. 1888 people smugglers were arrested, 2174 weapons and 96 tonnes of drugs seized, and 406 stolen cars detected. 134 potential victims of THB were able to be detected and 104 new criminal cases opened.

However, in the year 2022, the agency also faced a series of internal turbulences, including the resignation of the Executive Director (→eucrim news of 21 June 2022) and investigations by OLAF into serious misconduct on the part of Frontex (→eucrim news of 30 November 2022). Hence, in 2022, the agency implemented a series of changes:

- Strengthening of the Fundamental Rights Office;
- Creation of a network of fundamental rights focal points in all its entities in order to develop fundamental rights expertise in all areas of activity;
- Recruitment of 40 fundamental rights monitors;
- Establishment of internal audits for better governance, compliance, and accountability;
- Revision of the Serious Incident Reporting mechanism to improve the reporting on events at the external borders, including fundamental rights violations.

Ultimately, the well-being of staff and fostering a change in management culture within the agency was given priority. Finally, in December 2022, the Frontex Management Board appointed Lieutenant General *Hans Leijtens*, Commander of the Royal Netherlands Marechaussee, as the agency's new Executive Director. (CR)

Frontex' Joint Operation in North Macedonia

Based on the status agreement between North Macedonia and the EU, which entered into force on 1 April 2023, Frontex launched a joint operation at the external border of North Macedonia on 20 April 2023. With the help of more than 100 European border guards, the operation aims to strengthen and support the country's border management efforts. Under the command and control of the Border Police of North Macedonia, the European border guards will support local authorities with their border surveillance and border checks, including patrols, document checks, and information gathering on cross-border crime. Additionally, training activities will be conducted to further develop regional border control capacities. The Frontex joint operation hosted by North Macedonia is the fifth such operation hosted by a country outside the EU. (CR)

Irregular Border Crossings in 2022

On 13 February 2023, Frontex published the figures for irregular border crossings in the year 2022. With around 330,000 detected, irregular border crossings, the figure is the highest since 2016. In addition, the number had increased by 64% compared to 2021. Between 24 February 2022 and the end of 2022, almost 13 million Ukrainian refugees were counted on entry at the EU's external land borders from Ukraine and Moldova. In the same period, 10 million Ukrainian nationals were reported exiting at the same border sections. These numbers are not included in the figures mentioned above.

According to Frontex, 45% of all irregular entries in 2022 occurred via the Western Balkans. The Western Balkan and Eastern Mediterranean routes also saw the highest increase ever. Nationals of Syria, Afghanistan, and Tunisia were most frequently reported to have irregularly crossed or attempted to cross the EU's external borders. (CR)

Grant to Ukrainian Border Guards

On 23 January 2023, Frontex and the State Border Guard Service of Ukraine signed a grant agreement to support Ukrainian border officers in performing their duties during the winter months. The grant, which was signed remotely, is endowed with €12 million. It cov-

ers equipment used for civilian border management purposes at Ukraine's Western borders with EU Member States and Moldova and within its proximity. Relevant equipment entails, for instance, warm winter uniforms for border guards, electric generators, portable power stations, field kitchens, patrol vehicles, and pumps. (CR)

Specific Areas of Crime

Protection of Financial Interests

ECA Will Probe Effectiveness of Rule-of-Law Conditionality Mechanism

On 23 January 2023, the European Court of Auditors (ECA) announced that it has started working on an audit that will assess the effective application of the EU's conditionality mechanism to protect the EU's budget against rule-of-law breaches by Member States. The "general regime of conditionality for the protection of the Union budget" was introduced by Regulation (EU, Euratom) 2020/2092 of 16 December 2020 (→eucrim 3/2020, 174–176). Under certain conditions these rules require countries' access to EU funding to be suspended, reduced or restricted when there have been serious breaches of the rule of law. So far, the EU has only applied protective measures under the Regulation against Hungary (in December 2022 →eucrim news of 28 December 2022).

The ECA will examine whether the Commission has effectively applied the tools at its disposal to protect the EU's financial interests. The audit will focus on cohesion policy and the COVID-19 recovery funding and it will include six sample countries (Bulgaria, Greece, Italy, Hungary, Poland, and Romania).

ECA's audit preview does not include yet specific observations, conclusions or recommendations. The audit report is expected in about a year's time. (TW)

RRF Disbursements Break €150 Billion

On 31 March 2023, the Commission reported that it has meanwhile disbursed over €150 billion to EU Member States under the Recovery and Resilience Facility (RRF), which started 2 years ago. The funds are designed to contribute to the EU's economic recovery from the corona pandemic and to stimulate investment and reform. Under the RRF, Member States receive funding upon the successful completion of pre-agreed milestones and targets, which correspond to different stages in the roll-out of reforms and investments. Germany, for example, will receive €25.6 billion in grants from the RRF. They are intended, *inter alia*, to decarbonisation and digitalisation in the country.

As the implementation of the RRF progresses, the Commission also launched an online interactive map showing projects supported by the RRF and implemented on the ground by Member States. The aim of the interactive map is to enhance transparency on the functioning of the RRF and on its tangible impact for EU citizens, businesses, and civil society. The map allows to retrieve the following information:

- Geographical location of reform projects and investments in Member States and their state of play;
- Lead to more detailed information on the projects/investments provided online.

The map already includes over 100 reform projects that have been or are implemented in the Member States as well as over 250 investments.

The map complements other transparency tools on the RRF, such as the Commission website dedicated to the RRF, the Recovery and Resilience Scoreboard, providing regularly updated information on the disbursements and progress made by Member States, and the regular updates of the Member States' own portals, which are required by the REPowerEU Regulation. (TW)

ECA Warns of Gaps in the Control of the Recovery and Resilience Facility

spot light

On 8 March 2023, the European Court of Auditors (ECA) published a report in which it warns of gaps in the protection of the EU's financial interests and criticises the Commission's control system for the Recovery and Resilience Facility (RRF). The ECA took a closer look at the design of the Commission's control system for the RRF and how it fulfils criteria of assurance and accountability.

The RRF is the EU's large-scale financial support to Member States to overcome the corona pandemic and to stimulate investment and reform. The ECA first points out that the RRF follows a different spending model than the regular EU spending programmes do. Under the RRF, Member States receive funding upon the successful completion of milestones and targets, which are based on preliminary assessments by the Commission. Even though RRF-funded projects must comply with EU and national financing rules, such as procurement procedures and fulfilment of eligibility criteria for reimbursable costs, compliance with these rules are no precondition for making payments, unlike with other EU programmes. In this context, the ECA criticises that there is only limited verified information at the EU level on compliance with these EU and national rules, which impacts the assurance the Commission can provide and finally leads to a accountability gap at the EU level.

In addition, although there is an extensive set of checks for verifying the fulfilments of milestones and targets, the various stages in the preliminary assessment were insufficiently specified and not fully documented. It also

lacks a clear plan on the extent money should be frozen or reduced if targets and milestones are not fully fulfilled or if reform measures are reversed.

Regarding the protection of the EU's financial interests, the ECA notes that the Commission will audit the countries' own control systems to prevent, detect and correct fraud, corruption, conflicts of interest and double funding. However, this does not cover whether Member States adequately check the compliance of RRF-funded investment projects with EU and national rules and, if breaches occur, the EU money is duly recovered. Further shortcomings with regard to the protection of the financial interests result in the fact that the Irregularity Management System does not contain centralised and standardised information on fraud related to the RRF. Lastly, flat rate corrections to be applied in the event of a deficiency in Member States' control systems are insufficiently defined.

Against this background, the ECA addresses several recommendations to the Commission:

- Improving the procedures for *ex ante* verifications;
- Drawing up guidance on the reversal of a measure related to a previously fulfilled milestone or target;
- Addressing the EU-level assurance gap regarding the compliance of RRF-funded investment projects with EU and national rules;
- Aligning reporting on RRF-related fraud;
- Developing internal guidance regarding corrections, as provided for in the financing agreements.

The ECA announced that it also plans to look at the EU countries' checks in RRF spending.

The ECA has addressed several reports on the topic of RRF. Earlier, in January 2023, the auditors published a comparative analysis of the RRF and the EU's cohesion policy funding 2021–2027. It looks at the similarities and differences between both instruments in terms of their governance and management, programming of spending, conditions for making payments, monitoring and cost of implementation, control, and audit. For the RRF, the analysis already concluded that the Commission must ensure that the financial interests of the EU are effectively protected. (TW) ■

ECA Calls for Simplification and Better Accountability of EU's Complex Financial Landscape

On 1 March 2023, the European Court of Auditors (ECA) published a special report "The EU's financial landscape – A patchwork construction requiring further simplification and accountability". ECA auditors call for further simplification of the complex EU financial landscape and recommend making efforts for consolidation. They point out that the EU's current financial landscape has been described by the European Parliament as a "galaxy of funds and instruments surrounding the EU budget".

According to the report, over the past 15 years, more and more financial instruments have been created outside the EU budget, making the system overly complex and not fully publicly accountable. For some of these instruments, there is a gap in the audit of their performance and no control by the European Parliament.

One of the ECA's findings was that new instruments have been created in response to new policy challenges and to legal or practical constraints on the use of existing instruments. However, for most of the instruments examined by the ECA, it was not clearly documented that the chosen option and its design were the most appropriate solution, which would have been good practice.

The ECA also found that elements of the instruments, such as governance arrangements, sources of funding and the backing of liabilities, vary considerably, which increases complexity. The auditors address several recommendations to the Commission, including:

- Ensuring that any new instrument, which is proposed, contains an assessment of the design and options chosen;
- Compiling and publishing information on the EU's overall financial landscape;
- Making a proposal to integrate the Modernisation Fund into the EU budget;
- Proposing the integration and consolidation of existing financial assistance instruments.

Regarding audit control, the ECA states that it does not have the mandate to audit some instruments outside the EU budget and suggests that an ECA mandate should be established for all types of financing for EU policies. (TW)

ECA: Detection of Conflicts of Interests in Cohesion and Agricultural Spending Has Flaws

In a report, released on 13 March 2023, the European Court of Auditors (ECA) found loopholes in transparency and detecting situation at risk if it comes to conflicts of interests. ECA's report focuses on how conflicts of interests as an irregularity affecting the EU budget have been addressed in agricultural and cohesion policy – the EU's biggest spending areas.

One of the findings was that self-declarations are widely used at the national and EU levels, however this method has numerous disadvantages. For example, declarations can prove unreliable, and cross-checking the information can sometimes be difficult because of insufficient administrative capacity, data protection rules, and general difficulties associated with achieving full transparency. At EU level, "revolving doors" (staff moving from official public roles to private-sector roles in the same area) pose an increased problem.

Regarding the detection of conflicts of interests, the auditors remarked that the transposition of adequate rules to protect whistleblowers is still lacking. Lastly, they noted that there is no publicly available information about the scale of conflicts of interest in shared management of EU spending, and no indicators measuring the frequency or magnitude of the issue.

The ECA recommended measures to help the Commission improve its capacity to prevent and detect conflicts of interest and promote transparency. (TW)

Corruption

EP Pushes for Increased Transparency and Integrity after Qatargate

The European Parliament (EP) has pursued further steps in order to ensure better rules on transparency, accountability and integrity of the European institutions after allegations of corruption from Qatar had occurred in 2022 (→eucrim 4/2022, 242–243).

On 8 February 2023, European Parliament group leaders endorsed the reform plan, proposed by EP President *Roberta Metsola*, at the Conference of Presidents in Brussels. The reform plans address short-term measures and include, *inter alia*:

- A cooling off period for MEPs who wish to lobby Parliament when they are no longer in office;
- Mandatory registration in the Transparency Register for any event with participation of interest representatives in the EP;
- All Members, assistants and other staff, who have an active role on a report or resolution are required to declare scheduled meetings with diplomatic representatives of third countries, and with third parties covered by the scope of the transparency register (specific exemptions will be allowed);
- Revised declaration form on financial interests, that would include clearer information on Members' side jobs and outside activities;
- Reinforcement of cooperation with national authorities to boost the fight against corruption.

On 14 February 2023, the EP extended the task of the special committee on foreign interference (ING2), which is henceforth named "special committee on foreign interference in all democratic processes in the European Union, including disinformation, and the strengthening of integrity, transparency and accountability in the European Parliament". It will be tasked, among other things, with identifying the shortcomings in Parliament's rules on transparency, integrity, accountability and anti-corruption. ING2 will also have to propose measures for the medium- and longer-term and issue recommendations for reforms.

On 16 February 2023, the EP's plenary adopted two resolutions by which further improvements are called upon. The first resolution lists several follow-up measures on integrity, such as:

- Ensuring full implementation of the current rules on transparency and accountability in accordance of the Code of Conduct for MEPs, including financial sanctions for breaches of the Code of Conduct;
- Introducing more sanctionable activities into the Code of Conduct;
- Increasing transparency and accountability of NGOs by reviewing existing regulations in order to prevent NGOs from being used as vectors of foreign interference in European parliamentarism;
- Establishing additional vetting for parliamentary assistants and staff working on sensitive policy fields, particularly in foreign affairs, security and defence;
- Introducing a ban on MEPs who carry out remunerated side activities that could create a conflict of interest with their mandate;
- Obliging MEPs, their staff and Parliament employees to declare work meetings with third country diplomats, where they would have "an active role and clear and immediate influence" in Parliament's work, except where this could put those involved in danger or jeopardise public interest;
- Aligning internal rules with the Whistleblower Directive.

In its second resolution, MEPs call for losing no more time to establish an independent EU ethics body as already proposed in September 2021. The Commission is urged to submit a legislative proposal in this regard by the end of March 2023. The resolution finally outlines some elements and the structure of the new EU ethics body. According to the MEPs, the body should, *inter alia*, have the right to start investigations on its own and to conduct on-the-spot and records-based investigations. In addition, it should also have the possibility to check the veracity of declarations of financial interests and assets. (TW)

Handbook of Good Practices in the Fight against Corruption

spot light

On 15 February 2023, the European Commission published a Handbook of good practices in the fight against corruption. It was commissioned by the European Commission and drafted in a collaborative effort between the research team at the international research and consultancy company Ecorys and experts from the network of the Local Research Correspondents on Corruption (LRCC) in each Member State. It is based on desk research and 30 expert interviews conducted between April 2022 and October 2022.

The Handbook is designed to serve as a cornerstone for further improvement of national efforts to prevent and fight corruption and to stimulate peer learning and exchange between Member States. It is also seen as a tool that can inspire future research.

The Handbook describes 27 good practices, corresponding to one initiative per Member State, either a successful one or a promising new one. An anti-corruption practice was considered "good" if it 1) has a positive effect on countering corruption, and 2) demonstrates a mechanism that is transferable and applicable in other Member States. The handbook and the 27 good practices are structured around eight different themes, each containing a theoretical part and a part featuring case studies that focus on implementation, the estimated costs of a practice, its outcomes, and its limitations:

- Transparency & open data;
- Citizen engagement;
- Collective action;
- Integrity promotion;
- Conflict of Interest management and detection;
- Anti-corruption strategy;
- Anti-Corruption Agencies;
- Detection and investigation of corruption.

The Handbook demonstrates that the anti-corruption strategies used by EU Member States differ significantly. Preventive and repressive measures, internal governmental control and societal monitoring, and group action of many stakeholders are only a few examples of the differences. The analysis carefully examines the benefits and restrictions of each of these approaches.

According to the list of suggested best practices, a number of anti-corruption trends stand out:

- The goal of new transparency practices is to address issues of inconsistent or weak enforcement of freedom-of-information agreements, varying interpretations of transparency, and making public information both accessible and understandable to the general public;
- There are several efforts to create new data sets and combine data from different databases, including compulsory entries about companies and individuals (e.g. beneficial owners) – however, this brings challenges in terms of ensuring high-quality data, enforcing universal (not selective) obligations for transparency, and making large amounts of data understandable and useful to law enforcement agencies;
- Collaborative approaches, such as the engagement of citizens and other stakeholders, are visible, not only as an objective of many anti-corruption initiatives but also as an implementation mechanism for other outcomes (e.g., creation of anti-corruption strategy);
- Systemic, coherent initiatives on integrity – an important complementary approach to anti-corruption – have been established, which nonetheless are faced with challenges of ensuring effectiveness of the social norms of integrity and setting tangible goals;
- Anti-corruption strategies have been adopted and special anti-corruption agencies have taken up their work, but in future multi-stakeholder engagement in and decentralization of anti-corruption should be increased.

The Handbook forms part of the European Commission's overall anti-corruption policy and precedes a proposal for a directive on the use of criminal law to combat corruption. It also aims to support initiatives such as the experience-sharing workshops between the Commission and Member States' experts to discuss good practices in the fight against corruption. (AP) ■

Study: Need for Stronger Legislative Alignment of EU's Fight against Corruption

As a key deliverable of the EU's Organised Crime Strategy 2021–2025, the Commission published the study "Strengthening the fight against corruption: assessing the EU legislative and policy framework" on 3 January 2023. The study was carried out by EY and RAND Europe on behalf of the European Commission, Directorate-General Migration and Home Affairs (DG HOME). It aimed at providing recommendations for possible EU measures in the area of the prevention and repression of corruption by assessing and comparing the impacts of the policy options identified.

Overall, the evaluation identified legal and administrative obstacles that impede the EU's efforts to prevent and combat corruption. A lack of adequate data collection and monitoring of corruption data and corruption trends inhibits sufficient prevention of corruption in the EU, as do major disparities in the legislative and administrative frameworks in place at the national level to combat corruption.

Stronger legislative alignment among EU Member States in the fight against corruption, along with supportive soft measures, is the preferred policy option to address the issues identified. In order to increase the efficiency of investigations and the prosecution of corruption, the following measures are needed, according to the study:

- Minimum rules on the statute of limitations for corruption-related cases;
- Minimum rules on the immunity for members of the government or the parliament;
- Reverse burden of proof in asset confiscation related to illicit enrichment cases;
- Common minimum standards against enablers of corruption;
- Establishment of an EU anti-corruption prevention agency, including an EU anti-corruption coordinator;
- Development of an EU Corruption Index to counter the lack of data on and knowledge of the magnitude of corruption in the EU with prevention programmes.

The preferred policy options should be implemented by an EU Directive. (AP)

Money Laundering

Trilogue on AML Package Started

After the European Parliament (EP) approved its negotiating position in mid-April 2023, trilogue negotiations with the Council and Commission on the EU's anti-money laundering package

could start in May 2023. The Council set its position already in December 2022. The reform of the EU's rules on combating and preventing money laundering and terrorist financing was tabled by the Commission in July 2021 (→eucrim 2/2021, 153). The EP and Council will now debate on:

- The EU "single rulebook" Regulation, with provisions on conducting due diligence on customers, transparency of beneficial owners and the use of anonymous instruments, such as crypto-assets, and new entities, such as crowdfunding platforms. The EP also proposed including provisions on so-called „golden" passports and visas;
- The 6th Anti-Money Laundering Directive – containing national provisions on supervision and Financial Intelligence Units, as well as on access for competent authorities to necessary and reliable information, e.g. beneficial ownership registers and assets stored in free zones;
- The Regulation establishing the European Anti-Money Laundering Authority (AMLA) with supervisory and investigative powers to ensure compliance with AML/CFT requirements. (TW)

EDPB Urges EU Legislature to Halt Draft on Data Sharing for AML/CFT

On 4 April 2023, the European Data Protection Board (EDPB) sent letters to the trilogue partners (the European Parliament, the Council, and the European Commission) concerning the envisaged rules on data sharing for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes. The EDPB reacts to the Council's negotiating position of December 2022 on the new Regulation on AML/CFT (→ eucrim 4/2022, 246), which was proposed by the Commission in July 2021 (→ eucrim 2/2021, 154–155). The new Regulation on AML/CFT features directly applicable rules on the performance of customer due diligence by obliged entities and the reporting of suspicious activities or transactions, primarily to Financial Intelligence Units (FIUs).

The EDPB stressed that some of the provisions of the draft Regulation (Arts. 54(3a), 55(5), 55(7)) obliging entities or public authorities to share with each other personal data information on "suspicious transactions" and data collected in the course of performing their customer due diligence, pose risks to the fundamental rights to privacy and the protection of personal data. The EDPB expressed serious concerns as to the lawfulness, necessity, and proportionality of these provisions, recommending that the EU legislators not include them in the final text of the Proposal for a Regulation on AML/CFT. (AP)

Cryptocurreny Laundromat ChipMixer Taken Down

ChipMixer, an unlicensed cryptocurrency mixer, was taken down by German and US authorities on 15 March 2023, with help from Europol, Belgium, Poland, and Switzerland. The platform, which was set up in 2017, specialised in mixing/cutting trails related to virtual currency assets, making it attractive for money laundering activities.

Until its take-down, the platform had laundered an estimated 152.000 Bitcoins in crypto assets, worth roughly €2.73 billion according to current estimations. The platform was also used by ransomware actors to launder their ransom payments. On the action day, four servers, approximately 1909.4 Bitcoins (worth approx. €44.2 million), and 7 TB of data were seized. (CR)

Organised Crime

Criminal Infiltration of EU Ports

On 5 April 2023, Europol – together with the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven, and Rotterdam – published a joint analysis report looking into the risk and challenges that criminal networks in EU ports pose for law enforcement. The report details how the EU ports' infrastructures are infiltrated by organised crime, how illicit goods are trafficked and extradited from maritime containers, and how container reference codes are misappropriated in the ports of Antwerp, Hamburg/Bremerhaven, and Rotterdam. It also shows how corruption plays a key role in enabling the infiltration of ports.

According to one of the main points of the report, when the sheer volume of containers handled each year in EU ports (over 90 million) is set against the low percentage of containers that can be physically inspected (2–10%), the detection of illicit goods becomes extremely challenging. In addition, infiltration opportunities for criminal networks are manifold, due to the many public and private actors with access to port infrastructure and port information. Hence, criminal networks target logistics companies with corrupt actors and container shipments that are less likely to be inspected. To extract illicit goods from the ports, the modus operandi currently being used is „PIN code fraud", i.e. the use of misappropriated container reference codes: criminals obtain, by corrupt means, the container reference code of the container in which the illicit goods are concealed. Using this code, which is normally intended to confirm that the container can be released in the destination port and picked up by the client, criminals retrieve the container from the port terminal pretending to be the legitimate client.

While major EU ports are already looking into solutions to counter illicit goods trafficking by, for instance, changing procedures, developing more secure database systems, and implementing innovative technologies (e.g. combining imaging and artificial intelligence to increase the screening

rate of containers and goods), the report reveals that secondary EU ports are now likely to become the target of criminal networks. Furthermore, concerns have been raised that the planned connection of 328 EU ports to the Trans-European Transport Network (TEN-T policy) – the EU's policy for the development of coherent, efficient, multimodal, and high-quality transport infrastructure across the EU – could reinforce this trend.

For these reasons, the report calls for a common Europe-wide approach giving attention to regional aspects, including legislative initiatives to streamline security measures in ports. Preventive and investigative actions, such as public-private partnerships to involve all port actors, are also essential for tackling the infiltration of criminal networks in EU ports. (CR)

Hit against 'Ndrangheta

On 3 May 2023, an Action Day as part of an international operation resulted in the arrests of 132 'Ndrangheta mafia members, an Italian criminal network devoted to international drug trafficking, international firearms trafficking, and money laundering. The criminal network has massive investments in several countries. Supported by Eurojust and Europol, law enforcement authorities in Belgium, Germany, Italy, France, Portugal, Slovenia, Spain, Romania, Brazil, and Panama involved more than 2770 officers on the ground during the Action Day. They managed to raid multiple locations and seize several companies.

According to the press release by Eurojust and Europol, the international operation was the largest hit against the Italian poly-criminal syndicate to date. It was part of the EMPACT Operational Action 2.3 on 'Ndrangheta and the Sicilian mafia, the first EMPACT action led by the National Antimafia Directorate (Direzione Nazionale Antimafia) in which Europol and Eurojust are co-leaders.

Eurojust supported the operation by establishing and financing two joint investigation teams, by hosting several coordination meeting and by facilitating the execution of European Investigation Orders. Europol supported the investigations, inter alia, by providing intelligence and cross-match reports and by analysing encrypted communication of the suspects. (CR)

Hit Against Chinese Human Trafficking

At the beginning of February 2023, law enforcement and judicial authorities from Belgium, Germany, Poland, Spain, and Switzerland took down a sex trafficking ring in the biggest hit against Chinese human trafficking in Europe ever. The international prostitution ring kept hundreds of Chinese women trapped in debt bondage across Europe and forced them to work as prostitutes to pay off their debts. Victims were lured to Europe with the promise of a legitimate job. As a result of the successful operation, over 300 victims have been identified so far. Thirty-five individuals were arrested, including five Chinese nationals considered high-value targets by Europol due to their involvement in multiple, high-profile criminal activities in Europe (CR)

Cybercrime

Ransomwere Group "HIVE" Eliminated

An operation between 13 countries and Europol led to the takedown of the ransomware HIVE. Over the last several years, the malicious software was used to compromise and encrypt the data and computer systems of large IT and oil multinationals in the EU and the United States of America. Ransom payments led an estimated 1500 companies to lose almost €100 million. The ransomware was also used as a so-called „ransomware-as-a-service" (RaaS), allowing other ransomware groups to attack a wide range of businesses and critical infrastructure sectors, such as government facilities, telecommunication companies, the manufacturing industry, information technology, and the healthcare and public health sector (including hospitals). With the takedown of HIVE, law enforcement authorities were able to provide many victims with the necessary decryption keys, helping them regain access to their data. (CR)

Takedown of Crypto Exchange Platform Blitzlato

A joint action between law enforcement and judicial authorities from numerous countries led to the takedown of the digital infrastructure used by the cryptocurrency exchange platform Blitzlato. The action was led by French and US authorities and supported by Europol. The operation also involved authorities from Belgium, Cyprus, Portugal, Spain and the Netherlands. In the process, several members of the platform's senior management were arrested, crypto wallets worth about €18 million in cryptocurrency seized, and hundreds of accounts at other crypto exchanges frozen. Blitzlato is suspected of facilitating the laundering of large amounts of criminal crypto-assets and converting them into Russian roubles. (CR)

Genesis Market Taken Down

On 4 April 2023, Genesis Market – one of the most dangerous marketplaces selling stolen account credentials to hackers worldwide – was shut down and its infrastructure seized. Over two million people had been listed for the sale of their identities. Genesis Market sold so-called bots (applications that infect victims' devices through malware or account takeover attacks) to criminals, enabling them to gain access to all the data harvested by the bots, e.g. fingerprints, cookies, saved logins, and autofill form data. In addition, the criminals were

provided with the means of using the stolen data.

Operation Cookie Monster was led by the U.S. Federal Bureau of Investigation (FBI) and the Dutch National Police (Politie). It involved 17 countries as well as Europol and Eurojust.

The investigation was supported by Europol's European Cybercrime Centre (EC3) since 2019, which also coordinated the international activity with the help of the Joint Cybercrime Action Taskforce (J-CAT). Eurojust actively facilitated cross-border judicial cooperation between the national authorities involved and hosted a command centre during the parallel operations in 13 countries.

In order to see whether your information was part of a Genesis Market leak, a portal developed by the Dutch Police allows you to check whether your information has been compromised. (CR)

End of Monopoly Market

In a joint action conducted at the end of April and coordinated by Europol, together with authorities from nine countries from inside and outside the EU, "Monopoly Market" – an illegal dark web marketplace mainly for buying and selling drugs – was shut down. Altogether €50.8 million in cash and virtual currencies, 850 kg of drugs, and 117 firearms were seized. In addition, 288 suspects were arrested in the USA, UK, Germany, the Netherlands, Austria, France, Switzerland, Poland, and Brazil. Because law enforcement authorities also gained access to the lists of buyers, Monopoly Market customers across the globe are now at risk of prosecution.

Operation SpecTor built up on the takedown of the marketplace's criminal infrastructure by German authorities in 2021. Based on troves of evidence provided by the German authorities, Europol compiled intelligence packages to serve as a basis for further national investigations. Europol's European Cybercrime Centre also facilitated the information exchange and carried out data analyses to identify vendors on the dark web.

Operation SpecTor follows up on other EU law enforcement actions against illicit dark web markets, such as DisrupTor (2020); Dark HunTor (2021) and Hydra (2022). (CR)

Environmental Crime

"From the Hives": Results of the EU Action against Honey Adulteration

On 21 March 2023, the Commission communicated the results of the EU-coordinated action called "From the hives", led by the European Commission's Directorate-General for Health and Food Safety (DG SANTE). It also involved the national authorities of 18 countries that are part of the EU Food Fraud Network, the European Anti-Fraud Office (OLAF), and the European Commission's Joint Research Centre (JRC). The aim of the coordinated action was to assess the market prevalence of honey adulterated with sugar. The result of the operation showed that a significant proportion of honey imported into the EU probably does not comply with the provisions of the "Honey Directive" (Council Directive 2001/110/EC). Thanks to OLAF, 44 EU operators were investigated and seven sanctioned.

Investigations led by OLAF, consisting of on-site inspection, sampling, and close examination of computers and phone records, revealed complicity between exporters and importers. The malpractices included, for example, the use of additives and colouring, masking of the true geographical origin of the honey, and the use of sugar syrups.

Ville Itälä, Director-General of OLAF, commended the team effort necessary for the coordinated action:

"The key word was teamwork. The European Commission's Directorate-General for Health and Food Safety initiated and coordinated the entire action. OLAF investigated to help identify suspicious operators, performed on-the-spot checks with national authorities, acquired and analysed computer and phone records. Colleagues at the JRC analysed samples collected at borders in their laboratories to detect adulteration. National authorities were, as always, on the front line of checks and investigations on the ground. OLAF has investigated international food fraud before and I am very glad that we could lend our experience. The EU is an importer of honey as the internal demand is higher than our domestic production. It is important that we remain vigilant against any abuse. The most frequent type of fraud with honey happens via adulteration, meaning by adding cheap ingredients instead of keeping the honey pure. But we also found instances of origin fraud, with labels claiming false origins of the product. This action served to raise attention, call for order, and deter any fraudulent practices."

DG SANTE published a comprehensive report with the results of the action. It involved 16 EU Member States as well as Norway and Switzerland. (AP)

Procedural Law

Procedural Safeguards

ECJ: Individual Reasons Not Necessary for Telecommunications Surveillance

On 16 February 2023, the ECJ ruled on the individualisation of the obligation to state reasons for the judicial authorisation of telephone surveillance measures (Case C-349/21, *HYA and Others*). In the period from 10 April to 15 May 2017, the *Spetsializirana prokuratura* (Specialised Public Prosecutor's Office, Bulgaria) submitted seven

applications to the President of the *Spetsializiran nakazatelen sad* (Specialised Criminal Court), requesting authorisation to use telecommunication methods to intercept, record, monitor, and trace the telephone conversations of four persons suspected of having committed serious crimes.

The court President granted each of these applications on the day they were submitted and issued seven corresponding decisions authorising telephone tapping (so-called telephone tapping authorisations). On 19 June 2020, the Specialised Public Prosecutor's Office accused those four persons, together with a fifth person, of participating in an organised criminal gang for the purpose of enrichment, smuggling third-country nationals across Bulgarian borders, assisting them in illegally entering Bulgarian territory, and receiving/giving bribes in connection with these activities. The Spetsializiran nakazatelen sad, the referring court, decided to stay the proceedings and refer the following questions to the ECJ for a preliminary ruling:

- Is the practice of national courts in criminal proceedings – whereby the court authorises the interception, recording, and storage of telephone conversations of suspects by means of a predrafted, generic text template in which it is merely asserted, without any individualisation, that the statutory provisions have been complied with – compatible with Art. 15(1) of Directive 2002/58 read in conjunction with Art. 5(1) and recital 11 thereof (Directive on privacy and electronic communications)?
- If not, is it contrary to EU law if the national law is interpreted as meaning that information obtained as a result of such authorisation is used to prove the charges brought?

The ECJ held that a decision authorising telephone interception need not contain an individualised statement of reasons if the precise reasons why the court considered the legal requirements to have been complied with can be easily and unambiguously inferred from a cross-reading of the decision. In addition, the decision need not contain an individualised statement of reasons if the application for authorisation is made accessible to the person against whom the use of special investigative methods has been authorised after the authorisation has been given.

The Court of Justice of the European Union has already been confronted several times with preliminary references from the *Spetsializiran nakazatelen sad* concerning the compatibility of Bulgarian criminal procedure law with Union law. As from 27 July 2022, the *Spetsializiran nakazatelen sad* was dissolved and certain criminal cases (including the one at issue) transferred to the *Sofiyski gradski sad* (Sofia City Court). (AP)

Data Protection

ECJ: Systematic Collection of Biometric and Genetic Data Contrary to EU Law

The systematic collection of biometric and genetic data of any accused person in order for them to be entered in a police record is contrary to the requirement of ensuring enhanced protection with regard to the processing of sensitive personal data. This statement was made by the ECJ in its judgment of 26 January 2023 in Case C-205/21 (V.S.). The case concerned Bulgarian legislation on police records and data protection.

➤ *Facts and background of the case*

In the case at issue, criminal proceedings for tax fraud led to *V.S.* being accused of participation in a criminal organisation. V.S. opposed to consent to the collection of her dactyloscopic and DNA profile data for the purpose of creating a police record. According to Bulgarian law, the police authorities are empowered to take such data from any person "who is accused of an intentional criminal offence subject to public prosecution."

The *Spetsializiran nakazatelen sad* (Specialised Criminal Court, Bulgaria), which was called to enforce the data collection vis-à-vis V.S., had doubts as to whether the Bulgarian legislation applicable to such "creation of a police record" complies with EU data protection law and referred several questions on the interpretation of Directive (EU) 2016/680 "on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (in short: LED).

➤ *Findings of the ECJ: Restrictions on effective judicial protection proportionate*

The ECJ ruled that neither Directive 2016/680 nor the EU Charter of Fundamental Rights preclude national legislation under which the court is obliged to authorise the compulsory collection of biometric and genetic data from accused persons, even though it is not yet in a position to assess at that time whether there are actually reasonable grounds for suspicion against the accused person. The accompanying restriction of effective judicial legal protection is not disproportionate, provided that national law later guarantees effective judicial control of the preconditions of the accusation. Otherwise, there would be a risk of obstructing the course of criminal investigations and unduly restricting the ability of investigators to solve further criminal offences by means of a data comparison.

➤ *Right to presumption of innocence observed*

The right to the presumption of innocence also does not prevent such an obligation of the court: Firstly, the collection of data is limited to those persons whose criminal liability has not yet been established. Consequently, this collection could not reflect the

authorities' impression that these persons were guilty. Secondly, the fact that the court, which has to decide on the guilt of the person concerned, cannot assess at this stage of the criminal proceedings whether the evidence on which the accusation of that person is based is sufficient, constitutes a guarantee of observance of his or her right to be presumed innocent.

➤ *But: Systematic data collection without proportionality test unlawful*

However, Directive 2016/680 precludes national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution, without requiring the competent authority to verify whether the collection is also proportionate. The national legislation must provide for an obligation on the part of the authorities to verify and prove, on the one hand, whether or not the collection is strictly necessary for the attainment of the specific objectives pursued and, on the other hand, whether or not those objectives can be attained by measures which represent a less serious interference with the rights and freedoms of the data subject.

In this context, the ECJ argued that Directive 2016/680 is intended to ensure enhanced protection against the processing of sensitive data, which include biometric and genetic data, as such processing may present significant risks to fundamental rights and freedoms. The requirement stated therein that such processing is allowed "only where strictly necessary" must be interpreted as laying down stricter conditions for the lawfulness of the processing of such sensitive data.

According to the judges in Luxembourg, national legislation which provides for the systematic collection of data from any persons accused of an intentional offence is in principle contrary to that requirement. This approach could lead to the indiscriminate and general collection of data from the majority of accused persons, since the concept of "intentional criminal offence subject to prosecution" is particularly general and can be applied to a large number of criminal offences, irrespective of their nature, their gravity, the particular circumstances of those offences, their possible link with other ongoing proceedings, the criminal record of the person concerned or his/her individual profile.

➤ *Put in focus*

The ECJ's judgement in *V.S.* is the second within a short period of time to deal comprehensively with the interpretation of the "Law Enforcement Data Protection" Directive 2016/680 (→eucrim 4/2022, 251). It shows that the Directive is becoming increasingly important in data protection practice. Although the ruling concerns the specific legislation in Bulgaria, the ECJ's statements may also have impacts in other EU Member States. This relates firstly to registration practice for police records and secondly to the treatment of sensitive data by law enforcement authorities (Art. 10 LED). (TW)

EDPB Launches First Coordinated Enforcement Action

On 15 February 2023, the European Data Protection Board (EDPB) launched a coordinated enforcement action for the first time. The first coordinated enforcement action focuses on the use of cloud-based services by the public sector. Under the action, 22 supervisory authorities, including the European Data Protection Supervisor (EDPS), will address over 80 public bodies across the European Economic Area (EEA), including EU institutions. The action will cover a wide range of sectors (e.g. health, finance, tax, education, central buyers or providers of IT services) to explore the challenges they are facing with General Data Protection Regulation (GDPR) compliance when using cloud-based services. Based on the results, the supervisory authorities will decide on possible additional national supervision and enforcement actions. The insights gained may also feed into a targeted follow-up at the EU level.

The EDPB, established by the GDPR, is an independent European body that facilitates the consistent application of data protection rules throughout the EU and promotes cooperation between the EU's data protection authorities. It is composed of representatives from the EU national data protection authorities (national supervisory authorities) and the EDPS. Its secretariat is provided by the EDPS and based in Brussels. The coordinated enforcement action follows the EDPB's decision of October 2020 to set up a Coordinated Enforcement Framework (CEF). (CR)

Commission's Draft on US Adequacy Decision Faces Headwind

spot light

The European Data Protection Board (EDPB) and the European Parliament (EP) made critical statements to the Commission's draft adequacy decision for data transfer to the USA.

On 13 December 2022, the Commission proposed a draft adequacy decision regarding the EU-U.S. Data Privacy Framework (DPF). The DPF is designed to replace the former EU-U.S. Privacy Shield, which was declared invalid by the ECJ's judgment in *Schrems II* (→eucrim 2/2020, 98–99). The effect of the DPF would be that personal data can flow freely from the EU to the USA in the private sector. According to the Commission, an assessment of the US legal framework let conclude that the USA provides comparable safeguards to those of the EU, so that personal data can be exchanged between EU and US companies. The Commission above all took into account Executive Order 14086 on "Enhancing Safeguards for United States Signals Intelligence Activities", signed by US President *Joe Biden* in October 2022 as well as regulations adopted by the US Attorney General that complemented the Order. Both

acts were considered to meet the criticism voiced by the ECJ in *Schrems II*.

In its opinion on the draft adequacy decision of 28 February 2023, the EDPB expressed concerns and requests clarifications on several points The EDPB is an independent European umbrella body which brings together the national data protection authorities and the European Data Protection Supervisor and which has a right to scrutiny adequacy decisions pursuant to the GDPR. The EDPB welcomed substantial improvements such as the introduction of requirements embodying the principles of necessity and proportionality for US intelligence gathering of data and the new redress mechanism for EU data subjects. The EDPB sees, however, still numerous shortcomings in relation to certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism. The EDPB seeks clarification on these points and would appreciate it if not only the entry into force but also the adoption of the adequacy decision were made conditional on the adoption of updated policies and procedures to implement Executive Order 14086 by all US intelligence agencies.

In an EP resolution adopted on 11 May 2023, MEPs share the concerns of the EDPB. They point out *inter alia* that US legislation still does not provide for independent prior authorisation for collection of bulk data and lacks an "objective criterion capable of justifying" the government interference with privacy, as required by the ECJ. In addition, the resolution notes that the US intelligence community still performs the practice of electronic mass surveillance of EU citizens. The resolution sees also existing shortcomings in the Executive Order 14086. Against this background, the EP concludes that the EU-US Data Privacy Framework fails to create essential equivalence in the level of protection. The Commission is called to continue negotiations with its US counterparts which would provide the adequate level of protection required by Union data protection law and the Charter. The Commission should also not adopt the adequacy finding "until all the recommendations made in this resolution and the EDPB opinion are fully implemented".

It should be noted that the adequacy decision is an implementing act that is decided by the Commission itself (Art. 45 GDPR). The opinions by the EDPB and the EP are not binding for the Commission. However, they set a clear legal and political statement. A Commission official announced that the Commission may put forward a revised version of the adequacy decision before the summer break. (TW) ■

Ne bis in idem

ECJ: Double Prosecution of Criminal Organisation Possible

spot light

A Member State can exempt certain offences affecting its national security from the scope of the transnational ne bis in idem. This can also concern the offence of forming a criminal organisation in which the person prosecuted participated has engaged exclusively in financial crime, in so far as the action of that organisation intended to punish harm to the security or other equally essential interests of that state.

➤ *Background of the case*

This is the ECJ's reply on 23 March 2023 to a reference for preliminary ruling by the Higher Regional Court of Bamberg (Germany) in Case C-365/21 (*MR / Generalstaatsanwaltschaft Bamberg*). The case at issue concerns a large-scale cybertrading fraud that affected, *inter alia*, Austrian and German investors. MR, who allegedly acted as one of the ringleaders of this criminal organisation, was sentenced to four years of imprisonment in Austria and was to be surrendered to Germany for this investment fraud after having served part of the sentence. The German authorities argued in favour of another prosecution in Germany. They referred to Germany's declaration under Art. 55(1)(b) CISA providing, *inter alia*, that the Federal Republic of Germany is not bound to Art. 54 CISA (the transnational *ne bis in idem* principle) if the acts to which the foreign judgment relates constitute the offence of Sec. 129 of the German Criminal Code, entitled "Forming criminal organisations".

In the light of Art. 50 CFR, the referring court first wondered whether such a declaration is still valid. In the affirmative, it posed the second question of whether the requirements of Art. 55(1)(b) CISA are met if the criminal organisation engaged exclusively in financial crime. For further information →eucrim 3/2022, 193.

➤ *The ECJ's reply to the validity of Art. 55(1)(b) CISA*

In the first place, the ECJ confirms the validity of Art. 55(1)(b) CISA. The ECJ calls to mind that Art. 55(1)(b) CISA derogates from the principle of *ne bis in idem* where the acts to which the foreign judgment relates constitute an offence against the security or other equally essential interests of that Member State. Hence, it constitutes a (legitimate) limitation to the fundamental right guaranteed by Art. 50 CFR, which can be justified under the conditions of Art. 52(1) CFR. According to the judges in Luxembourg, Art. 55(1)(b) CISA respects the essence of Art. 50 CFR and the principle of proportionality as required by Art. 52(1) CFR.

Regarding the essence of the principle of *ne bis in idem*, it is argued that the exception in Art. 55(1)(b) CISA permits Member States to apply it to punish offences which affect the Member State itself and thus to pursue objectives that necessarily differ from those for which the person prosecuted has already been tried in another Member State.

Regarding proportionality, it is stressed that Art. 55(1)(b) CISA is an

appropriate option for achieving the general objective of punishment by a Member State of harm to its security or to its other equally essential interests. Moreover, the option for derogation is accompanied by rules guaranteeing that the disadvantages for the person concerned are limited to what is strictly necessary in order to achieve the objective.

➤ *The ECJ's interpretation of "security interests" in Art. 55(1)(b) CISA*

In the second place, the ECJ clarifies that "an offence against national security" as provided for by Art. 55(1)(b) can also cover offences whose constituent elements do not specifically include harm to the security of the Member States. Thus, the notion goes beyond offences which, by their very nature, relate to security, such as espionage, treason or serious harm to the functioning of public authorities. However, the offence in question must first affect the Member State itself and second particularly seriously affect it. A characterisation as an "offence against national security" must take into account the seriousness of the damage which its activities caused to that Member State. Under these conditions, offences that punish a criminal organisation that engages exclusively in financial crime, can fall under the derogation of Art. 55(1)(b) CISA. The judges in Luxembourg conclude however from the information made available to the Court that the criminal activities in the main proceedings have not had an effect of damaging the Federal Republic of Germany and thus are not covered by Art. 55(1))(b) CISA.

➤ *Put in focus*

The question on the validity of the reservations in Art. 55(1) CISA were already posed in the *Kossolowski* case (C-486/14), but remained unanswered by the ECJ to date. The ECJ now affirms such validity and recognises Art. 55 CISA as part of Union law that can limit the fundamental right in Art. 50 CFR. It is one of the seldom cases in which the judges at the bench at Kirchberg substantially disagree with the opinion by the Advocate General (AG). In the case at issue, AG *Szpunar* concluded that declarations under Art. 55(1)(b) CISA are incompatible with the CFR and provisions referred to in such declarations cannot be applied in judicial proceedings (→eucrim 3/2022, 193). He, *inter alia*, argued that the essence of the *ne bis in idem* principle is not respected. This result was already promoted by AG *Bot* in the said Kossolowski case.

The question remains, however, whether the ECJ will also apply these lines of argument to the other exceptions provided for in Art. 55(1) CISA, i.e. the possibility to make declarations if the acts to which the foreign judgment relates to took place in the territory of the Member State (lit. a) or were committed by its officials (lit. c). This can trigger further references for preliminary rulings also bearing in mind that the opinion of AG Bot in the Kosslowski case referred to Art. 55(1)(a) CISA, i.e. the territoriality clause. And here, the ECJ's developed argument that the criminal proceedings in two Member States pursue essentially different objectives is rather weak.

The second point of the ECJ's judgment in MR deserves attention, too. The Court interpreted the notion of "national security", which also may have impacts on other areas of Union law. Here, the Court did not only look at the nature of the offence, but above all took into account its effects. These must, of course, affect the state itself and be of a high degree of severity. Since the fraud in the main proceedings against MR only affected private investors, the application of Art. 55(1)(b) CISA was excluded. Conversely, the judgment let conclude that fraud committed by criminal organisations that is detrimental to several national budgets, for instance, may be prosecuted twice, if the second prosecuting Member State made a relevant declaration in accordance with Art. 55 CISA. Hence, the judgment in MR can have implications for the prosecution of offences against the EU's financial interests in the future.

It is now finally to the Higher Regional Court of Bamberg to apply the ECJ's answers to the given case. As the judges in Luxembourg indicated, it cannot be believed that the exception in Art. 55(1)(b) CISA applies since the criminal activities of the organisation have not harmed the Federal Republic of Germany notwithstanding the huge dimension of the fraud scheme. The Higher Regional Court of Bamberg must then apply Art. 54 CISA and mainly answer the question of whether the prosecution in Germany refers to the "same acts" which were subject to the conviction in Austria. Also in this respect, the ECJ provides hints in an exceptional preliminary remark at the beginning of the judgment. In this context, the judges in Luxembourg caution to look closely at the ruling of the Austrian court. Only if the ruling had considered the harm to persons residing in Austria, the German judicial authorities may conclude that the criminal proceedings in Austria did not relate to the same acts as those covered by the prosecution in Germany. In such scenario, the earlier decision may be considered to have been related to "similar acts", which is not sufficient to satisfy the "*idem*" condition in Art. 54 CISA. (TW) ■

AG: Volkswagen Cannot Be Penalised in Italy for "Dieselgate"

Advocate General *Campos Sánchez-Bordona* gave his opinion on the double jeopardy ban in connection with the sanctioning of Volkswagen (VW) due to the diesel scandal by the Italian authorities. On 30 March 2023, he delivered his opinion in Case C-27/22 (*Volkswagen Group Italia S.p.A. and Volkswagen Aktiengesellschaft*). The Italian Council of State (*Consiglio di Stato*) had asked whether a fine imposed on VW by the Italian competition and market surveillance authority, which had initially not

become final, violated the prohibition of double punishment under Art. 50 of the EU Charter of Fundamental Rights (CFR), since VW had in the meantime received a penalty order from the public prosecutor's office in Brunswick (Germany) in the same context, which became final through payment of the fine.

Due to the repressive purpose and the severity of the fine, the AG assumed the criminal nature of the Italian sanction in the case, even though it is classified as an administrative penalty under Italian law. The criminal nature is also true for the fine imposed in Germany. As a result, Art. 50 CFR was applicable. Furthermore, the fine imposed by the Italian authority and the German proceedings concerned the same legal person and the facts were identical in substance and in time, so that a violation of the prohibition of double punishment was to be affirmed in principle.

Therefore, the decisive question is whether an exception to the *ne bis in idem* principle could be justified in a constellation of cumulative sanction proceedings. Such exception must meet the requirements of Art. 52(1) CFR. According to the AG, the proportionality and necessity of the limitation are particularly problematic in the case. It can be inferred from the ECJ's case law that the following three criteria must be met:

- Clarity and precision of the rules giving rise to the duplication of proceedings and penalties;
- Coordination of proceedings in which a penalty is imposed, which must have a sufficiently close connection in substance and time so as to reduce to what is strictly necessary the additional burden associated with the duplication of proceedings of a criminal nature conducted independently;
- An assurance that the seriousness of the overall penalties imposed corresponds to the seriousness of the offence.

The AG observes that there has obviously not been a coordination between the Italian market surveillance authority and the German prosecution service of Brunswick. Hence, the AG doubts as to whether "it is possible (and realistic) to insist on that requirement in the event of the duplication of proceedings in which a penalty is imposed in two Member States, conducted by competent authorities in different sectors of activity, where there is no legal mechanism for coordinating those authorities' actions." However, the AG does not believe that the ECJ will reverse its previous case law.

The AG concludes that the prohibition of double punishment could not be permissibly restricted pursuant to Art. 52(1) CFR, because the coordination of measures between the authorities of the Member States, which is necessary to justify such a restriction, had not taken place.

Put in focus: Case C-27/22 was subject to a detailed analysis by *Laura Neumann* in her eucrim article of 27 March 2023 (in this issue). She came to the same result as the AG but with a different argumentation. It is now up to the judges in Luxemburg whether they will apply their previous case law, particularly developed in *Menci* (→eucrim 1/2018, 24–25), *bpost* and *Nordzucker* (both at →eucrim 2/2022, 116–118). By contrast to the other cases, the VW Dieselgate scandal case involves a duplication of proceedings between an administrative and a criminal law enforcement authority with a transnational dimension. (TW)

Victim Protection

Referral of 8 Member States to CJEU Over Protection of Whistleblowers

On 15 February 2023, the Commission decided to refer the Czech Republic, Germany, Estonia, Spain, Italy, Luxembourg, Hungary, and Poland to the Court of Justice for failing to transpose and notify national measures implementing the directive on the protection of persons who report breaches of Union law (Directive 2019/1937). The directive, which was adopted and entered into force in 2019, requires Member States to provide effective channels for whistleblowers working in the public and private sectors to report breaches of EU law in confidence and to establish a robust system of protection against retaliation. The referral of the eight countries comes in response to their unsatisfactory responses to the Commission's reasoned opinions. (AP)

Cooperation

Police Cooperation

Exchange of Information between Law Enforcement Authorities on New Footing

spot light

Following the provisional agreement in November 2022 (→eucrim 4/2022, 252–253), the Council and the European Parliament formally adopted the Directive on the exchange of information between the law enforcement authorities of Member States. The Directive (2023/977) was published in the Official Journal L 134 of 22 May 2023, p. 1.

It will repeal Framework Decision 2006/960/JHA on "simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union", known as the "Swedish Initiative".

The new Directive lays down the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.

➤ *Scope and use of evidence*

The Directive covers the exchange of information for the purpose of preventing, detecting or investigating criminal offences between the com-

petent law enforcement authorities of different EU Member States.

It does not apply to exchanges of information for said purposes that are specifically regulated by other Union legal acts. It does also not impose any obligation on Member States to (a) obtain information by means of coercive measures; (b) store information for the sole purpose of providing it to the competent law enforcement authorities of other Member States; and (c) provide information to the competent law enforcement authorities of other Member States to be used as evidence in judicial proceedings.

Regarding the latter point, the Directive also clarifies that it does not establish any right to use the information provided in accordance with this Directive as evidence in judicial proceedings. Even though they are not required to do so, Member States providing information under the Directive, however, are allowed to consent, at the time of providing the information or thereafter, to the use of that information as evidence in judicial proceedings.

➤ *Main features*

Key points of the Directive are Single Points of Contact established or designated by the Member States, to which requests for information must be submitted, the provision of information pursuant to such requests, the working languages of the Single Points of Contact, mandatory time limits for providing requested information and the reasons for the refusal of such requests.

The exchange of information under the Directive is made subject to five general principles:

- Availability;
- Equivalent access;
- Confidentiality;
- Data ownership;
- Data reliability.

➤ *Requests for information*

Rules on requests for information to the Single Points of Contacts include, for instance, the obligation for the submitting authority to carry out a necessity and proportionality test and be ensured that the requested information is available to that other Member State. In addition, the Directive lays down criteria when a request can be considered urgent as well as minimum (formal) requirements for the request in order to allow a rapid and adequate processing. Requests can be submitted by Single Points of Contact or designated Member States' law enforcement authorities.

➤ *Time limits*

Each Member State must ensure that its Single Point of Contact provides the requested information as soon as possible and in any event within the following time limits, as applicable: (a) eight hours in the case of urgent requests relating to directly accessible information; (b) three calendar days in the case of urgent requests relating to indirectly accessible information; (c) seven calendar days in the case of all other requests.

Deviation from the time limits is possible if a judicial authorisation is needed. In this case, the requested Single Point of Contact must keep the submitting authority updated and provide the requested information as soon as possible after obtaining the judicial authorisation.

➤ *Refusal grounds*

Regarding the important issue of refusing requests, the Directive first clarifies that refusal should be the exception. Refusal cases are to be specified exhaustively and interpreted restrictively. However, the rules set out in the Directive place an emphasis on the principles of necessity and proportionality, thereby providing safeguards against any misuse of requests for information, including where it would entail manifest breaches of fundamental rights. The Member States, as an expression of their general due diligence, should therefore always verify the compliance of requests submitted to them with the principles of necessity and proportionality and should refuse those requests they find to be non-compliant. Refusal grounds include the following:

- The requested information is unavailable;
- The request does not meet the minimum requirements as to its content (cf. above);
- The required judicial authorisation under national law was refused;
- The requested information constitutes personal data that falls outside the data categories in Annex II.B of Directive 2016/794;
- The requested information has been found to be inaccurate, incomplete or no longer up to date;
- The provision of information would harm or jeopardise important interests;
- The request pertains to:
  - (i) a criminal offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State; or
  - (ii) a matter that is not a criminal offence under the law of the requested Member State;
- There is no consent from another Member State or third country which initially provided the data to the requested authority.

➤ *Means of information exchange*

In order to allow for the necessary flexibility in view of operational needs that might vary in practice, the Directive provides for two other means of exchanging information, in addition to requests for information submitted to the Single Points of Contact. The first one is the unsolicited provision of information by a Single Point of Contact or by a competent law enforcement authority to the Single Point of Contact or a competent law enforcement authority of another Member State without a prior request, i.e. the provision of information on its own initiative.

The second one is the provision of information upon a request for infor-

mation submitted either by a Single Point of Contact or by a competent law enforcement authority *directly* to a competent law enforcement authority of another Member State. In respect of both means of exchange of information, the Directive sets out only a limited number of minimum requirements.

➤ *Language regime and communication channel*

The Directive includes an interesting provision on the language to be used for the exchange of information. Member States shall establish and maintain a list of one or more of the languages in which their single contact point is able to exchange information. This list should include English.

The default channel of communication will be Europol's Secure Information Exchange Network Application (SIENA). Following a proposal from the EP, SIENA will also be accessible to front-line officers on mobile phones.

➤ *Organisation of Single Points of Contact*

Chapter V of the Directive includes harmonised rules on the establishment or designation, tasks and capabilities of Single Points of Contact as well as their organisation, composition and training.

The Single Points of Contact must have access to all information available within their Member State, including by having user-friendly access to all relevant Union and international databases and platforms. It must also be ensured that Single Points of Contact carry out their tasks 24 hours a day, 7 days a week and are provided with qualified staff, appropriate operational tools, technical and financial resources, infrastructure, and capabilities, including for translation, necessary to carry out the tasks under the Directive in an adequate, effective and rapid manner.

Member States must also ensure that the Single Points of Contact deploy and operate a single electronic case management system (CMS). The Directive lays down certain minimum functions and capabilities of such CMS. The CMS is a workflow system allowing Single Points of Contact to manage the exchange of information.

➤ *Next steps*

The Directive entered into force on 12 June 2023. Member States must transpose the Directive by 12 December 2024. By way of derogation, Member States have time until 12 June 2027 to establish the secure communication channel of the Single Points of Contact with Europol's SIENA.

The Commission shall, by 12 June 2026 and every five years after 12 June 2027, submit a report to the European Parliament and to the Council assessing the implementation of this Directive by the Member States. On 12 June 2027, a first report from the Commission assessing the effectiveness of the Directive is due.

➤ *Put in focus*

The Directive forms part of the EU Police Cooperation Code package, by which the EU intends to enhance law enforcement cooperation across Member States and to give EU police officers more modern tools for information exchange. The package also contained proposals for automated data exchange for police cooperation ("Prüm II") and for a Council Recommendation on operational police cooperation (→eucrim 4/2021, 225–226). The legislative procedure regarding the revision of the Prüm framework is still ongoing. The Council Recommendation on "Law Enforcement Cooperation" was adopted in July 2022 (→eucrim 2/2022, 120).

Directive 2023/977 attempts to remedy flaws encountered by Framework Decision 2006/960. Evaluations showed that the Framework Decision ("the Swedish Initiative") has been scarcely used in practice, in part due to the lack of clarity. One crucial point in practice was unclarity between the Framework Decision and the use of judicial cooperation instruments, such as the Directive regarding the European Investigation Order (EIO). The new Directive on the exchange of information between law enforcement authorities does likely not solve this intricate point either. The question remains unclear of how information is to be exchanged that will subsequently be used as evidence in criminal proceedings. On the one hand, the Directive emphasises that it does not affect Union legal acts on cross-border evidence gathering, such as the EIO Directive and the future Regulation for electronic evidence. On the other hand, it allows the pure consent to the use of already submitted information as evidence in criminal judicial proceedings and vaguely remarks in Recital 14 that this consent *may* be achieved, "where necessary under national law, through the use of instruments regarding judicial cooperation in force between the Member States." It was already unclear under the "Swedish Initiative" under which circumstances and requirements this consent can be given; the Directive rather reinforces the impression that the consent for the use of evidence in judicial proceedings is only a rubberstamp by the authorities of the requested state circumventing the rules of the legislation on judicial cooperation.

The application of the refusal grounds in practice will be another crucial point for the Directive. Interestingly, the Directive words that also the requested law enforcement authority can perform a check of the necessity and proportionality of the information request and not only the requesting authority. This is interesting because such checks by the "executing authority" were to be avoided in other cooperation instruments, such as the European Arrest Warrant.

Unclear remains, however, to which extent the requested authority can deny requests that breach fundamental rights or essential Union values, such as the rule of law. The Directive

does not formulate an explicit refusal ground for fundamental rights under the ones listed in Art. 6(1), first sentence. It is only in the subsequent sentence 2 of Art. 6(1) that "Member States shall exercise due diligence in assessing whether the request for information submitted to their Single Point of Contact is in accordance with the requirements set out in Article 4, in particular as to whether there is a manifest breach of fundamental rights."

This formulation is problematic for two reasons: First, Art. 4 of the Directive concerns formal requirements and does not include information on possible fundamental rights breaches in substance. How should the requested authority become aware of fundamental rights infringements? Second, the question arises what means "*manifest* breach". Is it a reference to the ECJ's case law on the European Arrest Warrant (i.e. the so-called *Aranyosi Căldăraru* test)?

In addition, it will be questionable whether the requested law enforcement authority will afford the necessary "due diligence" in practice to probe requests. This is all the more true against the background that the requests have to be executed within short deadlines.

It can only be hoped that the Commission will also take these aspects on safeguards into account in its effectiveness analysis in four years' time. (TW)

Judicial Cooperation

Final Report on 9th Round of Mutual Evaluations

spot light

On 1 March 2023, the General Secretariat of the Council tabled the final report on the ninth round of mutual evaluations. The round was dedicated to legal instruments of mutual recognition in the field of deprivation or restriction of liberty. Evaluators looked into the legislation and practice of the EU Member States with respect to the following four instruments:

- Framework Decision 2002/584 on the European Arrest Warrant (FD EAW);
- Framework Decision 2008/909 on mutual recognition of judgments imposing custodial sentences;
- Framework Decision 2008/947 on the mutual recognition of probation measures and alternative sanctions;
- Framework Decision 2009/829 on mutual recognition to decisions on supervision measures as an alternative to provisional detention ("European Supervision Order").

The report includes recommendations to the Member States and EU institutions/agencies in order to further enhance application of the instruments under evaluation. It also highlights that there is currently no particular need for legislation at the EU level.

The report concludes that judicial cooperation among Member States based on the FD EAW and the FD on custodial sentences works well in practice. However, there is room for development in some key areas. The functional relationship and complementarity between these two instruments are quite complex, so that more clarity across the EU should be aimed for.

Regarding the FD EAW, the report stated, *inter alia*:

- The approach by some Member States to implement optional refusal grounds in the FD as mandatory ones impedes the proper functioning of judicial cooperation in criminal matters based on mutual trust;
- The executing judicial authority must have a margin of discretion when applying grounds for optional non-execution (in line with the ECJ judgment in Case C-665/20 PPU →eucrim 2/2021, 103–104);
- Regarding the recurring issues concerning the application of the proportionality principle, a significant improvement could be observed compared to the findings of the fourth round of mutual evaluations in 2009; however, proportionality checks by executing authorities are still carried out in few Member States, which conflicts with the principles of mutual recognition and mutual trust;
- There is a need to clarify the ECJ jurisprudence on the risks of inhuman or degrading treatment at EU level;
- Member States that are affected by bad detention conditions, including overcrowding, have taken or are considering initiatives to improve the situation;
- If surrender procedures are suspended or halted because of the *Aranyosi and Căldăraru* two-step test on detention conditions, efforts should be made by the competent Member States' authorities to avoid impunity.

Regarding FD 2008/909 on custodial sentences, the key findings were the following:

- Increased emphasis should be laid on the actual prospects of social rehabilitation for the sentenced person eligible for a transfer under the FD. Hence, the issuing authority should consult the executing Member State in order to gather the relevant information;
- Member States should ensure that their competent authorities inform the sentenced person about the possibility to serve the sentence in another Member State in accordance with the FD, the relevant procedure for the transfer and its legal implications, in a simple and accessible way;
- The issue of partial recognition and adaptation of the sentence does not raise major challenges, but problems remain in view of the interpretation of some notions in the FD and differences between the legal systems;

The ninth round of mutual evaluations confirmed that there is a significant lack of application of FDs 2008/947 and 2009/829 concerning non-custodial measures respectively

in the post-trial and pre-trial stages of criminal proceedings. Reasons are, for example, lack of awareness and knowledge among practitioners, complexity and length of the proceedings, and the low number of cases with cross-border implications. More specifically, the scant use of FD 2008/947/JHA is primarily due to the significant differences between national systems regarding the nature and duration of the applicable probation and alternative measures. The infrequent application of the European Supervision Order is usually linked to the difficulty in identifying appropriate cases. As a result, the report recommends raising awareness of these two FDs and providing guidance and tools for practitioners.

Lastly, the report assesses the cooperation with Eurojust and the European Judicial Network (EJN). It is concluded that both bodies could be involved more often in criminal cross-border cases. Therefore, Member States are encouraged to raise awareness and promote the use of Eurojust and the EJN and the tools they offer. (TW)

Commission Proposal for a Regulation on the Transfer of Criminal Proceedings

spot light

On 5 April 2023, the Commission presented a proposal for a Regulation on the transfer of proceedings in criminal matters between Member States (COM (2023) 185 final). The aim of the proposal is to generate more efficient criminal proceedings as well as better administration of justice within the EU. Up to now, there has been no uniform regulation under European law, so that a variety of problems arose, such as the constellation of parallel criminal proceedings in several Member States. The Commission expects that the new EU instrument will prevent the duplication of criminal proceedings as well as avoid impunity in case where surrender under a European Arrest Warrant is refused.

The Commission's proposal lays down common conditions for the transfer of criminal proceedings initiated in one EU Member State and to be transferred to another. It will, *inter alia*, be ensured that criminal proceedings are conducted in the best-placed Member State, for example, in the State where the major part of the crime occurred.

The proposal comprises five chapters with a total of 34 articles, which, in addition to general provisions, include the following:

- Common criteria for the transfer of proceedings as well as grounds for refusal to transfer;
- Time limits for deciding on the transfer of proceedings and costs of transfer;
- Obligations regarding the protection of the rights of suspects and accused persons as well as victims, possibilities of appeal against decisions to transfer;
- Effects of the transfer in the requesting and requested State;
- Admissible means of (in particular electronic) communication between the authorities involved;
- Final provisions, including provisions on statistics and the relationship with other international agreements/arrangements.

The Commission's proposal will now be discussed by the Council and the European Parliament before it can be finally negotiated in the trilogue. (TW) ■

Eurojust Report on Transfer of Proceedings in the EU

On 18 January 2023, Eurojust published its first report on the transfer of proceedings in the EU. The report examines the legal framework for the transfer of criminal proceedings in the EU, outlines the role of Eurojust in conflicts of jurisdiction and transfers of proceedings, and provides examples of recent challenges and best practices. The report is based on responses from Eurojust National Desks, the analysis of cases occurring between 2019 and 2021, and findings from previous reports.

The difficulties arising from the absence of a specific EU instrument regulating transfers of proceedings is one of the key issues identified in the report. It follows that EU Member States need to take recourse to a plurality of legal bases. Looking at the different national laws in this regard, the following obstacles exist:

- Differences regarding the notion of criminal proceedings;
- Different conditions, criteria, and grounds for not accepting a transfer of proceedings;
- Differences regarding who the competent authorities are for deciding a transfer of proceedings;
- Differences regarding the procedural safeguards granted to suspects and victims;
- Differences regarding legal remedies available to suspects and/or victims;
- The effects of the transfer of proceedings in the requesting State in which the criminal proceedings may be either closed or suspended.

Recurrent issues identified by the report include, for instance, the following:

- The (dis)agreement on which State is best placed to prosecute as well as existing limits under applicable national law;
- The involvement of central authorities, including lack of communication, the information to be transmitted with a request for transfer, translations, and practical issues regarding transfer of the case file;
- The involvement of suspects and victims;
- The coordination of provisional measures;
- The admissibility of evidence.

In its conclusions, the report makes the following recommendations:

- To hold informal preliminary consultations among the national judicial authorities involved before actually submitting a formal request for a transfer;
- To involve Eurojust during the entire life cycle of the case;
- To use Joint Investigation Teams (JITs), given their role in preventing conflicts of jurisdiction and in streamlining transfers of proceedings;
- To follow the examples of best practice outlined in the report with regard to practicalities for the transfer.

Lastly, the report calls for a new EU legal instrument to lay down common criteria and procedures for transferring criminal proceedings to another EU Member State and includes some proposals on the content of such an instrument.

The Commission is planning to launch a legislative initiative that will put in place common rules for transferring criminal proceedings between EU countries. (CR)

European Arrest Warrant

ECJ Upholds Restrictive Fundamental Rights Jurisprudence on the EAW in Catalan Surrender Cases

spot light

On 31 January 2023, the ECJ, sitting in for the Grand Chamber, published an important decision on the possible refusal of European Arrest Warrants (EAWs) due to fundamental rights concerns voiced in the executing state. The background of the case (C-158/21 – *Puig Gordi and Others*) are refusals by Belgian courts to surrender Catalan politicians who fled to Belgium after the illegal independence referendum in Catalonia in 2017. Belgian judges have been of the opinion that there was no legal basis according to which the Supreme Court in Madrid (*Tribunal Supremo*) was expressly authorised to decide and declined the execution of the EAWs due to the risk that the right to be tried by a tribunal previously established by law (Art. 47(2) CFR, Art. 6(1) ECHR) would be violated. Hence, in essence, the EAWs were refused because of a breach of the defendants' right to a fair trial.

➤ *Reference for preliminary ruling and AG's opinion*

The Spanish Supreme Court posed a series of questions to Luxembourg essentially asking whether the decisions by the Belgian courts were right. In addition, it asked how it can proceed with the cases, in particular whether it can maintain the existing EAWs or issue new ones after refusal of the execution of the EAWs on the grounds given. For more information on the preliminary ruling →eucrim 3/2022, 195–197.

In its opinion of 14 July 2022, Advocate General (AG) *Richard de la Tour* took the view that a judicial authority could not justify the non-execution of an EAW on the grounds of a possible violation of the requested person's right to a fair trial, unless systemic or generalised deficiencies in the judicial system of the issuing Member State were shown. (→eucrim 3/2022, 195–197).

➤ *The ECJ's judgment*

The ECJ follows the AG's argumentation. In essence, it decided that Belgian courts are not authorised to refuse the execution of an EAW by invoking a ground for refusal – in this specific case, the formal requirement of jurisdiction – which only arises from the law of the executing Member State. A refusal to execute EAWs is, however, (potentially) possible in the case of an obvious lack of jurisdiction in connection with a real danger of restrictions of fundamental rights and under the condition of systemic or generalised deficiencies affecting the judicial system of the issuing Member State. In more detail, the Court's argumentation was as follows:

➤ *ECJ on admissibility of the reference*

First, the ECJ clarified that the reference for preliminary ruling by the Spanish Supreme Court (the issuing authority) was admissible. Accordingly, the case should not be judged differently from the constellation in *AY* (Case C-268/17 →eucrim 2/2018, 105–106), where the issuing authority had been given the entitlement to let answer questions relating to the execution of EAWs by the executing authority. The judges in Luxembourg mainly argue that the referring court as the issuing authority has to decide on the maintenance or withdrawal of EAWs that may lead to the arrest of the fugitives and the observance of fundamental rights falls primarily within the responsibility of the issuing Member State.

➤ *ECJ on non-execution grounds beyond FD EAW*

As regards the merits of the case, the ECJ reiterated in the first place its settled case law on the main parameters of the EAW system, in short:

- Framework Decision (FD) 2002/584 on the European Arrest Warrant established a simplified and effective surrender system; its basis is the high level of trust between the Member States;
- To that end, it follows that execution of the EAW constitutes the rule, whereas the refusal to execute is the exception;
- The principle of mutual recognition works with the assumption that the EAW is issued by a "judicial authority";
- The executing judicial authority must not give effect to an EAW if the minimum requirements on validity (including those laid down in Art. 8 FD) are not met;
- The executing authority must or may refuse to execute an EAW only on the grounds set out in Arts. 3, 4, and 4a FD;
- On the basis of Art. 1(3) FD, the executing authority can refrain exceptionally and following an appropriate examination if a risk of infringement of fundamental rights set out in Arts. 4 and 47 CFR exists.

In this context, the ECJ emphasises that refusal grounds in the FD have a

strictly limited scope and a refusal can only be allowed in exceptional cases. Therefore, Member States cannot add other refusal grounds, because this would undermine the uniform application of the FD EAW. However, the judges in Luxembourg accept fundamental rights clauses in the implementation laws of the Member States (such as Art. 4(5) of the Belgian *loi du 19 décembre 2003 relative au mandat d'arrêt européen*) as long as they are interpreted in accordance with the respective ECJ case law on Art. 1(3) FD.

➤ *ECJ on refusal due to the concept of "judicial authority"*

In the second place, the ECJ clarified that its recent case law on the concept of "judicial authority" within the meaning of Art. 6(1) FD EAW (Joined Cases C-508/18 and C-82/19 PPU, *OG and PI* →eucrim 1/2019, 31–33) entitles the executing authority to examine that the EAW has indeed been issued by a "judicial authority", but not that the issuing judicial authority has, in the light o f the legal rules of the issuing Member States, jursidicion to issue an EAW. A distinct interpretation would confer the executing authority a general review function which would run counter the principle of mutual recognition.

➤ *ECJ on conditions to refuse due to fundamental rights infringements*

In the third place, the ECJ answers the central question on the conditions under which the executing judicial authority (here: the Belgian courts) may refuse to execute the EAW on the ground of an alleged infringement of the defendants' fundamental rights in the issuing country. The ECJ calls to mind its case law on fundamental rights checks in EAW proceedings. It particularly emphasises that the EAW mechanism is founded on the premiss that the criminal courts of the Member States, which will conduct the criminal procedure, are assumed to meet the requirements inherent in the fundamental right to a fair trial enshrined in Art. 47 CFR. Since the right is of cardinal importance, it can be safeguarded by the executing authorities, however, if the existence of a real risk is detected that the requested person, if surrendered to the issuing judicial authority, (will) suffer a breach of that fundamental right. To this end, it follows from the ECJ's case law that the executing judicial authority must carry out a two-step examination as follows:

- Determination of a real risk of infringement of the right at issue, on account of systemic or generalised deficiencies in the operation of the judicial system of the issuing Member State or deficiencies affecting the judicial protection of an objectively identifiable group of persons to which the person concerned belongs;
- Specific and precise verification whether – in the light of the concerned person's personal situation, the nature of the offence and the factual context – there are substantial grounds for believing that that person will run such a risk in the event of being surrendered to that Member State.

Subsequently, the judges in Luxembourg provide several clarifications on how the two-step examination should be carried out. Regarding the first step, they clarify that the determination of said deficiencies require an *overall assessment* of the operation of the judicial system of the issuing Member State in the light of the requirement for a tribunal established by law. These deficiencies are established if it is apparent that the defendants are generally deprived in the issuing Member State of an effective legal remedy that enables the review of the jurisdictional questions at issue either by an examination of the jurisdiction by the criminal court conducting the procedure or by another court.

Regarding the second step, it is clarified that the existence of a concrete risk can be established only if, in the light of the rules on jurisdiction and judicial procedure applicable in the issuing Member State, the court that will likely be called upon to hear the proceedings *manifestly* lacks jurisdiction.

In addition, the ECJ makes clear that the analyses pursuant to the two steps involves different criteria so that there is no overlap. As a result, the executing authority cannot refuse the EAW without having carried out both steps of the examination.

The judges in Luxembourg indicate that they do not see the first step to be fulfilled in the present case. In particular, given that the legal system of Spain provides for legal remedies enabling a review of the jursidcition of the *Tribunal Supremo* called to try the defendants, the risk of the breach of the fundamental right to be tried by a tribunal not established by law, can, in principle, be ruled out.

➤ *ECJ on loyal cooperation*

In the fourth place, the ECJ reiterates its case law that fundamental rights examinations by the executing judicial authority in the EAW scheme must be procdurally accompanied by a dialogue between the executing judicial authorities and the issuing ones. This follows from the principle of sincere cooperation and aims to avoid a standstill of the operation of the surrender system in the EU. As a consequence, Art. 15(2) FD EAW precludes the executing judicial authority from refusing to execute an EAW on the ground of a lack of jurisdiction of the trial court without having first requested that the issuing judicial authority provide supplementary information.

➤ *ECJ on successive EAWs*

Lastly, the Court rules that it is possible to issue several successive EAWs for a requested person with a view to obtaining his/her surrender by a Member State after the execution of a first EAW concerning that person has been refused by that State. However, the execution of a new EAW must not result in an infringement of the fundamental rights of that person

and the issuing of the new EAW must be proportionate.

➤ *Put in focus*

The judgment in *Puig Gordi and Others* is another landmark decision by the ECJ in the row of the controversial question to which extent the EU's surrender system enables objections against (potential) fundamental rights infringements by/in the issuing state. This question is also discussed under the heading "*ordre public* exception" in EAW cases. The ECJ makes repeating references to its decisions in *Openbaar Ministerie I and II* (judgment of 17 December 2020 in Joined Cases C-354/20 PPU and C-412/20 PPU →eucrim 4/2020, 290–291 and judgment of 22 February 2022, Joined Cases C-562/21 PPU and C-563/21 PPU →eucrim 1/2022, 33–34). In these decisions, the ECJ applied its case law on the interpretation of the EAW's fundamental rights clause inchoately regulated in Art. 1(3) FD 2002/584, which was first developed in relation of insufficient detention conditions (Joined Cases C-404/15 and C-659/15, *Aranyosi and Căldăraru* →eucrim 1/2016, 16), to fair trial interventions following the judicial reforms in Poland affecting EU's rule-of-law standards. By the *Puig Gordi* judgment, the ECJ now answers the open question left over after *Openbaar Ministerie I and II* as to how cases should be handled in which systemic or generalised deficiencies in the issuing state (such as bad prison conditions or attacks on the independence and impartiality of the judiciary) are not obvious at first sight.

The ECJ now makes unequivocally clear that its previous case law applies to all objections that certain fundamental rights standards are not maintained in the issuing EU Member State. It repeats its stance that a refusal for fundamental rights reasons can only be applied in exceptional cases. It emphasises in this context at several points in the judgment that a more lenient approach would affect the effective functioning of judicial cooperation between the EU Member States, thus recurring to the concept of "*effet utile*". Nonetheless, the judgment will not end criticism by scholars that this approach is too narrow and one-sided giving priority to effectiveness of cooperation over the individual's protection. This is corroborated by the ECJ's introduction of the element of a *manifest* lack of jurisdiction which can justify a refusal for fair trial reasons.

The criticism voiced by the author over AG *de la Tour's* opinion in the *Puig Gordi* case (→eucrim 3/2022, 197) must be maintained also after the final Court decision. In particular, the question remains of whether the ECJ's approach runs counter the "flagrant denial of justice" jurisprudence of the ECtHR in extradition cases. It is quite certain that a successful intervention of the person concerned with arguments of fundamental rights protection in the European Arrest Warrant system is extremely difficult, if not impossible.

At least, the ECJ answered the question that fundamental rights clauses or clauses of a European ordre public, which many EU countries have introduced into their national laws implementing Art. 1(3) FD EAW, are valid. This was also controversially discussed between proponents of a restrictive interpretation of refusal grounds (allowed only in the situations stipulated in Art 3, 4, and 4a FD) and their more protection-friendly opponents. Nevertheless, the Luxembourg judges impose a crucial restriction: The national laws must be interpreted in conformity with its case law on Art. 1(3) FD EAW, i.e. strict application of the two-step examination procedure as well as required dialogue between the executing and issuing judicial authorities.

Against the described background of the very restrictive approach to EAW matters, it remains to be seen whether national supreme / constitutional courts and the ECtHR will walk along with the colleagues at Kirchberg. (TW)

ECJ Rules on Suspension of European Arrest Warrant in Case of Serious Illness

spot light

By its judgment of 18 April 2023, the ECJ, sitting in for the Grand Chamber, added another important decision on the possibilities to suspend or refuse European Arrest Warrants (EAWs) in the event of fundamental rights problems. The Luxembourg judges decided that a manifest risk endangering the requested person's health can justify temporary suspension of his/her surrender. The executing judicial authority is obliged to ask the issuing authority for information concerning the conditions in which it intends to prosecute or detain that person.

➤ *Background of the case and AG's opinion*

The ECJ had to rule on a reference for preliminary ruling from the Italian Constitutional Court (Case C-699/21, *E.D.L.*). The referring court had to decide on an EAW from Croatia against E.D.L. An expert report revealed the existence of a psychotic disorder requiring medication and psychotherapy and it was said that E.D.L. is at increased risk of suicide if placed in a detention centre. The Italian Constitutional Court wonders in essence whether the ECJ's previous case law, which refers to the so-called Aranyosi test, can be extended, by analogy, to the situation of chronic illness of potentially indefinite duration, in order to avoid a serious harm to the peron's health. The referring court makes clear that the case at issue is different from the *Aranoysi/Căldăraru* case in which the ECJ developed its case law on the interpretation of Art. 1(3) FD EAW allowing the suspension of EAW due to fundamental rights infringements in the issuing state (Joined Cases C-404/15 and C-659/15, *Aranyosi and Căldăraru* →eucrim 1/2016, 16). According to the

Aranyosi test, systemic or generalised deficiencies in the issuing state as well as the realisation of a concrete danger of fundamental rights infringements in the issuing state are required. The Italian Constitutional Court particularly asked whether the Italian judicial authorities must enter into a dialogue with the issuing authority in Croatia and under which conditions Italy may even refuse the surrender of the requested person.

In its opinion of 1 December 2023, AG *Sánchez-Bordona* advised that the solution can be found in Art. 23(4) FD EAW, which stipulates that the surrender may exceptionally be temporarily postponed for serious humanitarian reasons. If necessary, the executing authority can postpone the surrender of the requested person for as long as serious health risks remains. The executing authority is obliged to communicate with the issuing authority (→eucrim 4/2022, 253–254).

➤ *The ECJ's judgment*

The ECJ follows the AG's opinion. It stresses that, on the basis of the principle of mutual recognition, a refusal to execute is to be understood as an exception and must be interpreted strictly. In principle, there is the assumption of an adequate health treatment of the requested person in the issuing state. It is nevertheless apparent from Art. 23(4) FD EAW that, in exceptional circumstances, relating, *inter alia*, to the life or health of the requested person being manifestly endangered, surrender may be temporarily postponed. The executing authority is therefore entitled to verify whether the execution of the arrest warrant manifestly risks endangering the health of the requested person, if there are substantial grounds, based on objective material, in this respect. The discretion must be exercised in accordance with Art. 4 CFR, which prohibits, *inter alia*, inhuman and degrading treatment.

If the executing judicial authority concludes that there are substantial and established grounds for believing that the surrender would expose the person concerned to a real risk of a significant reduction in his or her life expectancy or of a rapid, significant and irreversible deterioration in his or her state of health, it must postpone that surrender and ask the issuing judicial authority to provide all information relating to the conditions under which it intends to prosecute or detain that person and to the possibility of adapting those conditions to his or her state of health in order to prevent such a risk from materialising.

If, after this assessment, this risk cannot be ruled out within a reasonable period of time, the executing authority must exceptionally refuse the EAW.

➤ *Put in focus*

The *E.D.L* case supplements the ECJ's case law on the interpretation of Art. 1(3) FD EAW and the refusal of EAWs due to the European ordre public. As the AG, the judges in Luxembourg acknowledge that the cases of a refusal based on illness must be treated slightly differently as the cases decided to date in the context of Art. 1(3). In the latter cases, the ECJ had to decide on potential infringements by the issuing state, be it because of providing bad prison conditions (cf. the *Aranyosi and Căldăraru* decision above) or be it because of not guaranteeing a fair trial before an independent and impartial court ("*LM*" decision →eucrim 2/2018, 104–105). By contrast, in the E.D.L case, the concern over fundamental rights already existed in the executing state, i.e. the risk of infringing the defendant's right to life if surrendered. Other constellations in this regard would be possible infringements of the right to family life (Art. 7 CFR) if close family or social connections are interrupted by the surrender.

Hence, the "Aranyosi test" had to be adapted. Although the ECJ renounces the two-step examination as established in *Aranyosi and Căldăraru*, the Court sticks to its line of argumentation that refusal to execute EAWs due to potential fundamental rights infringements can only happen under exceptional circumstances. It is the executing judicial authority's task to ensure, by means of communication with the issuing authority, the exclusion of fundamental rights risks and give priority to surrender. In the cases of illness, the second preferred option must be the postponement of surrender. The final refusal of surrender can only be considered as the very last resort. (TW) ■

European Investigation Order

ECJ: EIOs by Tax Authorities Need Validation

In its judgment of 2 March 2023, the ECJ clarified that a German tax office responsible for criminal matters and tax investigation (*Steuerfahndung*) cannot issue European Investigation Orders (EIOs) without a judge, a court, an investigating judge or a public prosecutor having validated the EIO in advance.

➤ *Background of the case and legal question*

The underlying Case C-16/22 (*MS v Staatsanwaltschaft Graz*) concerns a question referred by the Higher Regional Court of Graz (Austria). The main proceedings deal with the issuing of an EIO on suspicion of tax evasion by the Düsseldorf Tax Office for Criminal Tax Matters with regard to the provision of information and transmission of documents relating to the Austrian bank accounts of a defendant. The defendant appealed against the decision of the Graz Regional Court to grant enforcement of the EIO. Since the tax office was not a judicial and issuing authority within the meaning of Directive 2014/42, she claimed that it lacked competence to issue the EIO.

The referring Higher Regional Court of Graz pointed to the complex German law under which the tax authorities are vested with the power to conduct criminal investigations autonomously

with regard to certain specified criminal (tax) offences. In this case, the tax authority assumes the rights and the obligations of the public prosecutor's office. However, a public prosecutor can take over the case at any time and without a specific reason. The Higher Regional Court wondered whether the German tax office responsible for criminal tax matters can claim to be regarded as "judicial authority" within the meaning of Arts. 1(1) and 2 (c)(i) of the EIO Directive.

➤ *The ECJ's ruling*

The ECJ emphasised that the Directive draws a clear distinction between Art. 2 lit. c (i), which exhaustively lists judges, courts, investigating magistrates and public prosecutors as judicial authorities, and Art. 2 lit. c (ii), which covers any other authority. Given that Art. 2 lit. c reflects the distinction, inherent in the principle of separation of powers, between the judiciary and the executive, already the wording indicates that tax offices must be examined pursuant to the second category (Art. 2 lit. c (ii)).

In addition, the Directive precludes a functional interpretation by which the German tax offices for criminal tax matters are equated with public prosecution offices if they are vested with the rights and obligations of the latter. This would not only be counter to the distinction between executive and judicial authorities but also give rise to legal uncertainty. This is not compatible with the objective of the EIO Directive, i.e. to establish a simple and effective cooperation scheme for gathering evidence.

As a result, the German tax offices as administrative authorities can be classified as an issuing authority, provided that the requirements of Art. 2 lit. c (ii) of Directive 2014/42 are met, i.e. it is necessary that the EIO issued by it is validated by a judicial authority before being transmitted to the executing authority.

➤ *Put in focus*

The question, which was now decided in substance, was already on the agenda before the ECJ. However, the previous reference for a preliminary ruling by the prosecutor's office of Trento (Italy), was declared inadmissible in September 2021 (→eucrim 2/2021, 162). In this case (C-66/20), the AG came to the same conclusion as the ECJ now in the case in Graz (→eucrim 1/2021, 37). (TW)

Law Enforcement Cooperation

E-evidence Framework: State of Play

At the end of January 2023, the representatives of the Council and the European Parliament agreed on the compromise text for the Regulation on cross-border access to electronic evidence in criminal proceedings and the accompanying Directive on the designation and appointment of legal representatives for the gathering of e-evidence. The compromises were reached in interinstitutional negotiations, which end a five-year long debate on the draft legislation. It was initially tabled by the Commission in April 2018 (→eucrim 1/2018, 35–36).

The new EU instrument seeks to introduce an alternative – quicker and more efficient – mechanism to the existing international cooperation and mutual legal assistance tools in order to specifically address the problems stemming from the volatile nature of e-evidence and the "loss of location" aspect of stored data.

Through the introduction of European e-evidence preservation and production orders, judicial authorities in one Member State will be able to request electronic evidence – both subscriber, traffic and content data – directly from a service provider in another Member State via a decentralised IT system. As a rule, the time limit to respond to a production order is ten days, in emergency cases eight hours. If a service provider does not comply with the order, sanctions of up to 2% of the annual worldwide turnover may be imposed.

The enforcing state is to be informed by notification and given the opportunity to assert reasons for refusal within ten days or, in emergency situations, 96 hours. This notification requirement does not apply if the offence was committed or will probably be committed in the issuing state and/or the person whose data is requested resides in its own territory.

After the finalisation of the EU rules on e-evidence, the Commission announced on 2 March 2023 that it resumed negotiations with the U.S. Department of Justice on the EU-U.S. agreement facilitating access to electronic evidence in criminal investigations. Negotiations started in September 2019 (→eucrim 3/2019, 179–180) but were put on hold while waiting for the EU legislation. (TW)

Council Frames Ratification of CoE E-evidence Treaty by EU Member States

On 14 February 2023, the Council adopted a decision that authorises EU Member States to ratify, in the interest of the EU, the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention). The Second Protocol regulates the cross-border exchange of electronic evidence in criminal proceedings (→eucrim 4/2021, 234). The Council's decision was published in the EU Official Journal L 63 of 28 February 2023, p. 48.

The decision paves the way for Member States to act jointly when ratifying the Protocol since only states can do so and not the EU itself. The annex of the Council Decision includes a number of reservations, declarations, notifications and communications in relation to the Protocol that Member States must make to ensure compatibility of the Protocol with Union law and policies. This includes the indication to Member States that participate in the enhanced cooperation on the European Public Prosecutor's Office (EPPO), that they should ensure the EPPO's

ability, in the exercise of its competences as provided for in Arts. 22, 23 and 25 of Regulation (EU) 2017/1939, to seek cooperation under the Second Protocol in the same way as national prosecutors of those Member States.

On 5 April 2022, the Council authorised Member States to *sign* the protocol, acting jointly in the interest of the EU (→eucrim 2/2022, 128). The Council also sent the decision to authorise Member States to ratify the protocol to the EP for consent as required under Art. 218(6) TFEU. The EP gave its consent on 17 January 2023 (→eucrim 4/2022, 254). (TW)

Criticism of New EU Plan for International Border Data-Sharing System

Ten civil society organisations submitted their criticism of the new Commission initiative "Security-related information sharing – reciprocal access for frontline officers in the EU and key partner countries". Among the dangers cited: aiding political repression and underpinning human rights violations.

The objective of the Commission's proposed plan is to create a single European channel for frontline officers in all Member States to have systematic and immediate access to security-related information from partner countries (provided by all Member States). This new system of information exchange would exist alongside existing channels (bilateral or multilateral agreements between Member States, EU and partner countries, Europol cooperation agreements, Schengen Information System (SIS) alerts based on information from partner countries, Interpol systems, the Prüm framework, etc.). Its aim is to create a tailor-made EU system for sharing „critical and actionable data" between frontline officers (e.g. border guards, police forces) in the EU and key partner countries. The Commission launched a public consultation on the plan in January 2023. The adoption of a legislative initiative is planned for the fourth quarter of 2023.

The ten civil society organisations argued that the Commission has failed to demonstrate why the new initiative to share information between EU and non-EU States is necessary, especially since a number of existing initiatives have already been criticised for jeopardising asylum procedures and the safety of third-country nationals seeking protection from corrupt regimes in EU Member States. The organisations therefore urgently asked that the Commission not go ahead with the initiative. (AP)

2022 JHAAN Activity Report

On 23 February 2023, CEPOL, in its capacity as outgoing Presidency of the EU Justice and Home Affairs Agencies' Network (JHAAN), published the final activity report for the year 2022. Agencies in the network include CEPOL, EIGE, EMCDDA, EUAA, eu-LISA, Eurojust, Europol, FRA, and Frontex (→eucrim 1/22, 35–36).

As the first Presidency of the newly established Trio Presidency (with CEPOL holding the Presidency in 2022, EUAA in 2023, and eu-LISA in 2024), CEPOL focused on implementation of the recommendations of the 2021 JHAAN Assessment Report. Emphasis was also placed on the joint priorities of the Trio Presidency for the years 2022–2024, i.e. digitalisation, business continuity, and implementation of the principles of the European Green Deal. Russia's military aggression in Ukraine had a strong impact on the year's activities.

As of 1 January 2023, the European Union Agency of Asylum (EUAA) has taken over the Presidency of the JHAAN. For the year 2023, in addition to continuing to support Ukraine, the priority topics defined by the EUAA include the following:

- Digitalisation;
- Implementating the EU Green Deal in Justice and Home Affairs Agencies;
- Cybersecurity;
- Providing information in mixed migration situations;
- Increasing communication and improving general awareness of the JHAAN network. (CR)

Council of Europe

Reported by Dr. András Csúri (AC)

Foundations

European Court of Human Rights

ECtHR: Key Developments in 2022

On 26 January 2023, ECtHR President *Síofra O'Leary* presented a summary of the Court's activities and its statistics for 2022. The exceptionally serious events of the year, namely the invasion of Ukraine, the exclusion of Russia from the CoE, and the loss of its status as a High Contracting Party to the Convention have had significant legal consequences. At the end of 2022, some 74,650 applications

were pending before the Court, 74% of which involved five countries: Turkey, the Russian Federation, Ukraine, Romania, and Italy. Important applications included
interstate cases, which the Court would give priority to. Almost 10,200 pending applications concerned conflicts between two Member States, i.e. Russia/Ukraine, Armenia/Azerbaijan, and Georgia/Russia. Of the total number of pending applications, some 23,850 were classified as priority cases because they raised important issues, for example under Art. 3 of the Convention.

Síofra O'Leary also called to mind that the ECtHR has been applying a new case management strategy since 2021 that aims at processing legally complex and often "sensitive impact" cases. In 2022, impact cases were decided, for instance, on sexual harassment in the workplace, freedom of expression of judges, and euthanasia.

Among other significant developments, on 1 February 2022, the time limit for bringing a case before the ECtHR under Protocol 15 to the Convention was reduced to four months from the date of the final domestic decision (→eucrim 1/2022, 39). Furthermore, the dialogue between the Court and the superior courts of the CoE states was strengthened. The network of higher courts has now grown to the remarkable figure of 103 courts in 44 countries.

Lastly, 2022 brought the launch of the external version of the Court's knowledge-sharing platform (ECHR-KS), which is now available to the public. The platform presents the latest analysis of case-law developments in a thematic and contextualised manner through particular Convention Articles and transversal themes. It is available in English and French and complements existing information tools such as HUDOC. Its content is updated on a weekly basis but is not binding on the Court.

ECtHR: Amendments to Rules of Court and New Guidelines on Third-Party Intervention

On 20 March 2023 the ECtHR published a new version of the Rules of Court on its website. They clarify third-party intervention in amendments to Rule 44 (2) and (3) (b). These rules govern the conditions and time limits for the submission of written comments or participation in hearings by the Commissioner for Human Rights, by contracting parties not party to the proceedings, and by persons other than the applicant. The amendments were adopted by the Plenary of the Court on 3 March 2023 and entered into force on the same day.

On the basis of Rule 32 and in parallel, the President of the ECtHR issued a Practice Direction on how third parties may intervene, the procedures and requirements to be followed, and the role such intervention plays in the work of the Court. The guidelines are linked to Art. 36 (2) ECHR, which concerns third-party intervention other than that of the Contracting Party to the proceedings or the applicant in applications before the ECtHR. In addition, Art. 3, second sentence of Protocol No. 16 allows any other High Contracting Party or person to take part in advisory-opinion proceedings.

The Practice Direction provides comprehensive guidance on the following:

- The role of third-party intervention in the Court's procedure;
- What third-party intervention involves;
- The stages in the proceedings before the Court when third-party intervention is possible, and the time limits for seeking leave to intervene in each possible scenario;
- Who may intervene as a third party under these provisions;
- When a third party is invited or permitted to intervene;
- The representation of third parties;
- The language, content, and manner of requesting leave to intervene;
- The requirements to be met by the written comments and oral submissions of the interveners.

ECtHR: Guidelines for Future Processing of Applications against Russia

Since the Russian Federation ceased to be a party to the ECHR on 16 September 2022 (→eucrim 3/2022, 199), the European Court of Human Rights (ECtHR) has ruled in a number of cases. In a background brief of 3 February 2023, the Registrar of the Court set out some guiding procedural principles for the future handling of cases against Russia that fall within the Court's jurisdiction:

- The ECtHR is competent to deal with cases concerning acts or omissions that took place before 16 September 2022, the date on which Russia ceased to be a party to the ECHR (*Fedotova and Others v. Russia*; *Kutayev v. Russia*; *Svetova and Others v. Russia*);
- Given that the office of the Russian ECtHR judge has ended, the Court will appoint an *ad hoc* judge from among the sitting judges to examine the cases lodged against Russia within its jurisdiction (*Kutayev v. Russia* and *Svetova and Others v. Russia;* Grand Chamber decision *Ukraine and the Netherlands v. Russia*);
- The Court may proceed with the examination of applications even though the Russian authorities do not cooperate with it, for example by not submitting written observations, as in the case of *Svetova and Others v. Russia*. This does not, however, automatically lead to acceptance of an applicant's claims.

On 1 February 2023, 16,730 applications lodged against Russia were pending before a decision body. There are also eight inter-State cases pending against Russia, which remain a top priority for the Court.

Specific Areas of Crime

Corruption

GRECO: Fifth Round Evaluation Report on Bulgaria

On 19 January 2023, GRECO published its fifth round evaluation report on Bulgaria. The focus of the fifth round is on preventing corruption and promoting integrity in central governments, especially regarding persons with top executive functions (PTEFs) and law enforcement agencies. In particular, the evaluation tackles conflicts of interest, the declaration of assets, and accountability mechanisms. Bulgaria has been a member of GRECO since 1999 and has fully implemented the recommendations of the first and second evaluation rounds, 70% of the recommendations of the third evaluation round, and 84% of the recommendations of the fourth evaluation round.

The perceived level of corruption in the country is high. According to the Corruption Perception Index published by Transparency International, Bulgaria ranked 78th out of 180 countries in 2021.

Bulgaria's anti-corruption framework is based mainly on the Law on Countering Corruption and Forfeiture of Unlawfully Acquired Assets, which has been in force since 2018 and contains provisions on the transparency and integrity requirements applicable to public officials as well as on the institutional framework to supervise implementation. At the time the report was adopted, the Anti-Corruption Law and the institutional setup of specialised bodies were in the process of being reformed.

Among Bulgaria's specific problems, according to the report, is the lack of a proper integrity framework for top officials of the government. There is no code of ethics applicable to them, no awareness raising on integrity matters, nor any established mechanism for confidential counseling. In addition, there is a lack of rules and transparency in respect of interaction with lobbyists seeking to influence government policies. The verification of top officials' declarations of interest and assets is also ineffective, as it is limited to desk analysis and cross-checking against information contained in other state databases. GRECO calls for more transparency concerning government officials, including their remuneration and possible ancillary activities. The response of criminal justice to corruption offences involving top government officials is ineffective: procedural impediments should be eliminated and adequate sanctions provided.

With regard to law enforcement authorities, it is necessary to prevent undue political influence, as the police and the Ministry of Interior are closely related, with the Minister having far-reaching powers over the police. GRECO recommends that a comprehensive code of ethics brings together provisions on ethics and the integrity required of police officers and covers matters such as conflicts of interest, gifts, contacts with third parties, outside activities, and handling confidential information.

There is a need for a sufficiently transparent procedure as regards recruitment and promotion procedures in the police force, for more representation of women at all levels, for an obligation to report integrity-related misconduct, and to ensure effective protection of whistle-blowers.

GRECO: Fifth Round Evaluation Report on Ireland

On 16 February 2023 GRECO published its fifth round evaluation report on Ireland. The country joined GRECO in 1999 and has implemented 75% of the recommendations of the first evaluation round, 85% of the second evaluation round, and 70% of the third evaluation round. Following the fourth evaluation round, only 45% of the recommendations were fully implemented, 20% partly implanted, and 35% not at all yet. According to the report, some aspects of the recommendations that remain to be addressed concern members of parliament and are also problematic for persons with top executive functions (PTEFs).

The perceived level of corruption in the country is low and stable. According to the Corruption Perception Index published by Transparency International, Ireland ranked 13th out of 180 countries in 2021.

The Standards in Public Office Commission (Standards Commission) is an independent body that plays a central role in the promotion of integrity standards and the prevention of conflicts of interest in respect of a wide range of public officials, including ministers, the Attorney General, special advisers, and senior civil servants. The Standards Commission has published guidance in several relevant areas such as conflicts of interest, gifts, and lobbying after leaving government. Due to the unique position of this body, GRECO calls for reinforced resources and powers to supervise the implementation of integrity standards.

The report states that, although there are a number of prevention policy documents, they lack the necessary focus on the specific exposure of PTEFs to corruption. It underlines that any risk assessment and subsequent policy should pay particular attention to PTEFs, that integrity checks should be carried out before they join government, and that systematic briefings and/or training on integrity should be organised after their appointments.

There are already integrity standards in legislation and guidance on them, but the report calls for codes of conduct geared towards PTEFs, covering relevant topics such as conflicts of interest, secondary activities, gifts, and post-employment restrictions. There should be more transparency when it comes to contacts with lobby-

ists and third parties, including regular, publicly available meeting reports by the PTEFs themselves.

Regarding the Irish police service (*An Garda Síochána*), the report calls for the already existing code of ethics to be supplemented to cover all relevant integrity topics – illustrated by real-life examples – , in particular conflicts of interest, gifts, contacts with third parties, secondary activities, and confidential information. The Garda information technology systems need to be further strengthened to better monitor integrity breaches by Garda members, and regular checks on authorized secondary activities are necessary to prevent the occurrence of conflicts of interest over time.

GRECO: Fifth Round Evaluation Report on Austria

On 1 March 2023, GRECO published its fifth round evaluation report on Austria. The country has been a member of GRECO since 2006, implementing 67% of the recommendations of the joint first and second evaluation rounds and 76% of the recommendations of the third evaluation round. After the fourth evaluation round, 16% of recommendations were fully implemented, 47% partly implemented, and 37% not implemented so far; the compliance procedure is still ongoing.

Austria traditionally scores high in perception surveys on the fight against corruption. According to the Corruption Perceptions Index of Transparency International it occupied the 13th rank in 2021out of 180 countries. Despite this, there has been a sharp increase in corruption cases in Austria over the last few years. This is partly due to the recent spike in high-profile scandals affecting the highest levels of the executive, involving former ministers, a vice-chancellor and a chancellor: in the latter case, raising questionable links between politicians, polling companies, and the media.

A national anti-corruption strategy has been in place since 2018, accompanied by a two-year action plan. Various key reforms are currently awaiting further development, however, with the prevention and management of conflicts of interest being a heightened challenge in Austria. At the central government level, there is no system in place to strategically analyse the main corruption risks persons with top executive functions (PTEFs) face. For ministers and state secretaries, there are some requirements on outside activities as well as financial interests and disclosure requirements, but there is room for improvement, particularly with regard to "revolving door" standards.

There is also need for greater transparency in the management and operation of state secretaries and ministerial advisers. The adoption of a specific law on access to information remains an outstanding issue.

PTEFs do not enjoy immunity from criminal prosecution, but the Central Public Prosecutor's Office for Combating Economic Crime and Corruption (WKStA) is subject to a reporting obligation in high-profile cases of public interest. This is time-consuming for prosecutors and can pose risks to the confidentiality, efficiency, and independence of criminal proceedings.

In Austria, law enforcement consists of the prosecution authority (including the WKStA, which was subject to GRECO's fourth evaluation round) and the criminal investigation authority, in particular the police and the Austrian Federal Bureau of Anti-Corruption (BAK). Several mechanisms have been developed to prevent corruption and enhance integrity in the police service, including the creation of positions for corruption prevention, compliance, and integrity officers. However, efficient risk management and risk analysis systems have yet to be put in place, and it is essential that senior officials are specifically targeted, as it appears that most of the current measures are aimed at low-level and mid-level officials. There are serious concerns about politization within the police, in particular regarding recruitment to senior level posts. Transparency needs to be increased and undue influence in the selection process avoided by improving the appointment system, including with regard to the management of the BAK.

A Code of Conduct for the staff of the Ministry of the Interior was first developed in 2010 and is regularly updated, the latest version dating from 2021. It takes a very practical and instructive approach, as it is coupled with advisory and awareness-raising channels. Effective mechanisms need to be developed to ensure proper application, however, and monitoring of the relevant rules and awareness-raising initiatives in this area need to be significantly stepped up.

Breaches of conduct provisions may lead to administrative/criminal responsibility under the relevant disciplinary/criminal law. To ensure uniform disciplinary action across the board, a federal disciplinary authority was established in 2021. As no specific statistics are kept on criminal or disciplinary proceedings for corruption involving law enforcement officials, further transparency is needed in this respect.

More efforts are also required to protect whistleblowers. Austria is currently drafting specific legislation on whistleblower protection to transpose EU Directive 2019/1937 on whistleblowing, a priority issue that requires immediate action.

GRECO: Fifth Round Evaluation Report on Bosnia and Herzegovina

On 9 March 2023 GRECO published its fifth round evaluation report on Bosnia and Herzegovina (BiH). The country joined GRECO in 2000 and initially had a positive track record of implementing GRECO recommendations; how-

ever, the trend has been declining. While 83.3% of the recommendations were ultimately implemented after the first evaluation round, full implementation of recommendations declined to 43.7% in the second and to 45.4% in the third evaluation rounds. Since the fourth evaluation round, the compliance procedure is still ongoing, as none of the recommendations have been fully implemented, and BiH has been in a non-compliance procedure since 2020.

This trend is reinforced by the general perception that corruption is widespread in BiH. The country has dropped from the 72nd position in 2013 to the 110th in 2021 in the Corruption Perceptions Index of Transparency International.

In recent years, there have been many obstacles at different levels of government. No state-level budget was adopted in 2021 and the first two quarters of 2022 and, due to this blockage, the country's institutions have been operating on a provisional budget for 16 months. As a result, Bosnia and Herzegovina's institutions are largely paralysed, legislative performance is non-existent, and reforms, including those needed to move towards EU membership, are stalled. In particular, the draft law on the prevention of conflicts of interest and amendments to the law on public procurement are pending.

The report notes that there is currently a "legal vacuum" in terms of corruption prevention policies in BiH. The 2020–2024 Anti-Corruption Strategy and its Action Plan have not been adopted to date, and a more holistic anticorruption policy at state-level is lacking. At present, there is no specific strategy to prevent corruption and promote integrity amongst persons with top executive functions (PTEFs). While the Code of Conduct for Civil Servants applies to advisers, no separate code of conduct for PTEFs exists in general. The relevant provisions (conflicts of interest, gifts, access to confidential information, etc.) are set out in different laws. In addition, the Agency for the Prevention of Corruption and Coordination of the Fight against Corruption (APIK) lacks the capacity to carry out its tasks properly and independently and is hardly operational.

The report recommends the development of an operational corruption prevention action plan based on a risk assessment specifically targeting PTEFs. More generally, clear guidance on conflicts of interest and other integrity issues should be included in the code of conduct of PTEFs, accompanied by appropriate monitoring and enforcement mechanisms. Rules should be put in place on how PTEFs interact with lobbyists and other third parties seeking to influence government decision-making. Regular and systematic information and the training of PTEFs on these standards should be organized.

The report calls for an independent review of the legislation governing freedom of information in order to address problems such as the lack of responsiveness of public authorities to requests for information. Increased transparency in the legislative process, in that external inputs and their origins should be identified, should be documented and disclosed.

The system for managing conflicts of interest for PTEFs also needs to be reviewed: their declarations of interest need to be subject to regular substantive checks. Proportionate sanctions for breaches should be in place, including for false reporting or failure to report. All PTEFs, whether elected or not, should be subject to the same disclosure requirements and, for the sake of transparency and accountability, all declarations need to be systematically, easily, and publicly available online.

As regards law enforcement, a system of regular anti-corruption action plans must be ensured, with clear objectives based on identified risks and an external evaluation of their implementation. The existing codes of ethics of the Border Police and State Investigation and Protection Agency should be complemented by practical guidance illustrating all issues and risk areas with concrete examples.

Both new and existing staff should be required to undergo ethics and integrity training based on practical guidance. Security checks on the integrity of police officers should also be carried out at regular intervals throughout their careers, and a system of asset declaration should be introduced.

Measures should also be taken to further promote a more balanced gender representation in all positions. In addition, a legal provision defining conflict of interest with police duties should be adopted, and authorised secondary activities should be duly registered. Lastly, the protection of whistleblowers needs to be reviewed and strengthened.

GRECO: Closure of *ad hoc* Procedure in Respect of Slovenia

On 26 January 2023, GRECO welcomed in a report the Slovenian Constitutional Court's decisions that parliamentary inquiries into particular judicial proceedings and decisions by judges and prosecutors were unconstitutional, as they risked violating judicial independence. The case concerned a parliamentary inquiry that had been set up to investigate possible politically motivated decisions by officials, prosecutors, and judges involved criminal proceedings as well as possible violations of fundamental rights under the ECHR. The State Prosecutor General of Slovenia subsequently filed a request for constitutional review on the unlawfulness of such legislative intervention in the judiciary (→eucrim 1/2020, 32).

On 18 February 2020, GRECO had published an *ad hoc* report on Slovenia under Rule 34 of its Rules of Procedure, which can be triggered in exceptional cases if reliable information is avail-

able on institutional reforms, legislative initiatives, or procedural changes that may lead to serious violations of CoE anti-corruption standards. GRECO closely followed the assessment of the situation in order to draw conclusions from the case as regards the adequacy of anti-corruption and integrity framework. Following the decisions of the Slovenian Constitutional Court in 2021 declaring the inquiries unconstitutional, these were annulled.

In its current report, GRECO noted that the Slovenian Constitutional Court has called on the Slovenian Parliament to establish additional safeguards and remedies to prevent such infringements in the future. The adoption of GRECO's report closes the *ad hoc* procedure in respect of Slovenia.

Money Laundering

MONEYVAL: Fifth Round Evaluation Report on Monaco

On 23 January 2023, MONEYVAL published its fifth-round evaluation report on the Principality of Monaco, based on an onsite visit concluded in March 2022. The fifth evaluation round builds on previous MONEYVAL assessments by strengthening the examination of how effectively Member States prevent and combat money laundering (ML) and terrorism financing (TF).

The report states that Monaco demonstrates a moderate level of effectiveness in relation to the following issues:

- ML/TF risk understanding;
- International cooperation;
- The application of AML/CFT preventive measures in the private sector;
- The use of financial intelligence;
- Implementation of the United Nations targeted financial sanctions (TFS) on TF and proliferation financing (PF).

Major improvements are needed regarding the transparency of legal persons, the effectiveness of supervision, ML investigations and prosecutions, and confiscation of proceeds of crime. The country has undertaken efforts to identify ML/TF risks, but some sectors such as those involving casinos, company services providers, trusts, and virtual assets as well as organised crime-related and external ML threats have not yet been adequately addressed.

The Monegasque Financial Intelligence Unit (Financial Channels Supervisory and Monitoring Service, SICCFIN) has a significant lack of human and technical resources but still produces high-quality analyses, which are not fully used however by the investigative authorities. Most Suspicious Transaction Reports (STRs) come from banks, with the contribution from professionals in other at-risk sectors still limited.

Monaco needs to enhance its efforts to identify and prioritize ML cases, especially seizing, confiscating, and recovering the proceeds of ML and predicate offences. There is a need to fundamentally improve the supervisory system, where there are deficiencies in relation to beneficial ownership. Also, the shortcomings in risk understanding undermine authorities' capacity to apply tailored supervision for a number of obliged entities.

The private sector has implemented the AML/CFT obligations to some extent. According to the report, the number of STRs originating from the banking sector is satisfactory, but the large volume of defensive reporting and excessively long transmission times raise questions about their quality. The designated non-financial businesses and professions (DNFBPs) have a poorer AML/CFT risk understanding and compliance culture. The number of STRs filed by casinos and jewellers is still limited, even though the two sectors play an important role in the principality.

The number of ML investigations and prosecutions remains modest. While they appear to be consistent with Monaco's risk profile, there are gaps relating to complex cases in particular. This is primarily due to an inadequate number of parallel financial investigations.

Monaco has secured convictions for ML involving the proceeds of crime generated abroad and standalone ML convictions. This does not cover ML committed by third parties, however, which is a significant deficiency given Monaco's status as an international economic and financial centre. The sanctions put in place are proportionate but not effective or dissuasive. The number of confiscation measures ordered is still low and they do not concern property of corresponding value or property held by third parties.

The principality's legal framework is appropriate for the implementation of TF- and PF-related TFS at the international, European, and national levels. As of May 2021, however, delays in the transposition of designations impacted the effectiveness of the mechanisms. The existing awareness-raising and supervision measures could no longer be regarded as proportionate and targeted. That there have been no convictions or prosecutions for TF in Monaco, which appears to be due to the shortcomings of the TF risk analysis, may not be consistent with the country's risk profile.

There is a good understanding of ML/TF risk associated with the activities of various types of legal persons, but there are major shortcomings in obtaining information on beneficial ownership. The mitigating measures applied are insufficient when a high-risk category of legal persons is involved and in relation to the non-for profit organisations. Most of the applicable sanctions on leagal persons are not dissuasive and are rarely imposed.

Major improvements are also necessary regarding the principality's effective contribution to international cooperation. Monaco generally seeks

the cooperation of its counterparts, although not entirely in line with the risk and context of the jurisdiction. The prosecution authorities execute requests satisfactorily, but systemic and unusual legislative obstacles hinder Monaco's provision of mutual legal assistance. As far as extradition is concerned, the restrictive interpretation by the courts of the dual criminality principle results in one out of two requests being refused.

MONEYVAL: Fifth Round Evaluation Report on Estonia

On 25 January 2023, MONEYVAL published its fifth-round evaluation report on Estonia based on an onsite visit concluded in May 2022. Among other things, the report encourages the country to reinforce the capacities and performance of the private sector and improve its law enforcement efforts in the field of AML/CFT. MONEYVAL acknowledges that Estonia has demonstrated a substantial level of effectiveness in international cooperation, the use of financial intelligence, and implementation of the United Nations targeted financial sanctions on proliferation financing.

Estonia has an appropriate mechanism in place for the identification, assessment, and, subsequently, understanding of ML/TF risks: national risk assessments with access to all data available in the country from public and non-public sources. While the results provide useful glimpses of sectors with higher risk exposure, they do not give a fully sufficient view of the risk environment. All competent authorities have a role in the implementation of the activities under the relevant national policy, but the outcomes of nationwide risk assessment exercises have not been integrated into the objectives and activities of individual authorities.

National cooperation and coordination is a strong feature of the country's AML/CFT regime, and MONEYVAL commends Estonia for the practice of co-ordination and co-operation between the Estonian Financial Intelligence Unit (EFIU) and the law enforcement authorities (LEAs). At the same time, a number of the EFIU's practices compromise the detection of crime and the tracing of assets, such as face-to-face meetings with the affected party to obtain further clarification on suspicious transactions, or lengthy suspension orders that result in the customer being notified of the application of the measure.

In view of its current heavy reliance on the LEA's leadership, there is also need for a moderate improvement of the EFIU's capacities and working practices when reinforcing its proactive approach in detecting ML/TF targets. According to MONEYVAL this is a priority issue for Estonia, given the EFIU's powerful position to observe and detect the movement of illicit flows.

More efforts are required on the part of the Supreme Court to improve the current interpretation of the ML offence, which is one of the main reasons for the relatively low number of identified and investigated ML cases. The criminal sanctions applied for ML offences call into question their dissuasiveness and effectiveness. Confiscation is recognized as a policy objective, but the proceeds of crime in specific cases were much higher than the amounts subject to confiscation. Moreover, Estonia does not proactively pursue proceeds moved abroad and sanctions applied for undeclared cash are minor.

The authorities undertake investigations into TF and have achieved one conviction, which does not fully correspond to the risk profile of the country. One of the reasons for this is the deficiency in TF risk understanding. While authorities use a range of sources of information when identifying and investigating TF, information published by the EFIU and its financial investigations could be better used to identify potential TF offences.

Significant improvement was achieved in the implementation of preventative measures during the assessment period, as a result of focused supervisory actions. The understanding of ML/TF risks is good in the banking sector. Virtual assets service providers (VASPs) and Company Service Providers (CSPs) demonstrated a superficial understanding of the ML risks to which their individual businesses are exposed. Understanding TF risk is generally lower across all sectors. Banks and VASPs generally have a good understanding of their AML/CFT obligations, while CSPs only have a lesser degree of understanding. Therefore, MONEYVAL expects continued efforts on the part of the supervisory authorities to strengthen the implementation of preventative measures in the private sector. The competent authorities have the power to access information, but the measures to prevent misuse of legal persons do not fully enable the availability of adequate, current, and accurate information on beneficial ownership.

The large share of Estonian companies with e-Residents as their basic or beneficial owners, significant involvement of licensed and non-licensed CSPs in the company registration processes, coupled with poorly designed and vaguely understood customer due diligence measures, are factors having an adverse impact on the quality of information on beneficial ownership. Applicable sanctions are not effective.

Estonia has reserved the right to refuse assistance based on the dual criminality principle with regard to non-EU countries. The country otherwise generally provides timely and constructive assistance across the range of requests for international cooperation, including mutual legal assistance.

Procedural Law

Victim Protection

ECtHR: Grand Chamber Reinforces Protection of Whistleblowers

With its Grand Chamber judgment of 14 February 2023 in the case *Halet v. Luxembourg* (application no. 21884/18), the ECtHR put an end to the long-lasting legal battle between one of the whistleblowers who triggered the LuxLeaks scandal and the state of Luxembourg. While previous judgments denied the defence of whistle-blower status according to Art. 10 ECHR (freedom of expression), the ECtHR's Grand Chamber decided in the opposite and found a violation of Art. 10 ECHR. The LuxLeaks scandal concerned tax agreements (resulting in tax avoidance) between multinational companies and the Luxembourg fiscal authorities. Mr *Halet*, one of the two whistleblowers, disclosed confidential documents protected by professional secrecy to journalists while he was employed by a private company. Luxembourg courts sentenced him to a €1000 fine and the Luxembourg Court of Appeal concluded that public interest in the disclosure was insufficient to outweigh the damage suffered by the private employer.

The ECtHR was called to decide whether Mr Halet's criminal conviction, following the disclosure of confidential documents issued by his employer, had amounted to a disproportionate interference with his right to freedom of expression. Under Art. 10 ECHR and the criteria established in *Heinisch,* employees may enjoy whistleblowers protection when disclosing in-house information, including secret information if strong public interest is involved. In a chamber judgment of 11 May 2021, the ECtHR had concluded that Mr Halet's criminal conviction did not constitute a breach of his right to freedom of expression arguing that public interest had been insufficient to counterbalance the harm caused to the company (→eucrim news of 21 June 2021).

In overturning this decision, the ECtHR's Grand Chamber now found that public interest in the disclosure outweighed all of the detrimental effects arising from it, given the importance, at both the national and European levels, of the public debate on the tax practices of multinational companies. It reasoned that the information disclosed by the whistleblower had made an essential contribution to the public's interest in receiving the information on tax rulings. Therefore, the interference with the applicants' right to freedom of expression, in particular his freedom to impart information, had not been "necessary in a democratic society" and thus violated Art. 10 ECHR.

Articles

Articles / Aufsätze

Fil Rouge

Artificial intelligence (AI) – machine-based systems that are guided by a set of human-defined goals – make predictions, suggestions, or decisions based on available data. They have begun to play a prominent role in many facets of our digital age, influencing everyone's lives. This fast-developing field of technology has huge potential to aid a variety of businesses and societal endeavors, but it could pose new risks and have negative consequences for people or society. The EU is currently debating the "AI Act", the first law on AI by a major regulator, which already sparked controversy on the right way. Against this background, the benefits and drawbacks of AI need to be carefully considered. The following articles examine the role of AI in law enforcement and legal proceedings in the EU and the challenges of contemporary Internet legislation.

In the first article, *David Hadwick* outlines the use of AI and machine learning systems by EU Member States in the area of tax enforcement and addresses the risk that particularly coercive AI tax enforcement systems may pose. He openly criticises the lack of clarification in the forthcoming EU AI Act regarding the treatment of AI tax enforcement systems and their possible classification as high-risk AI. Due to the specific nature of AI tax enforcement systems and the ambivalent nature of tax administration, he finds the distinction between administrative and law enforcement purposes in recital 38 of the draft AI Act particularly problematic.

Athina Sachoulidou, Dimitrios Kafteranis, and *Umut Turksen* present the TRACE project in a second article. TRACE deals with the development of AI solutions to identify, track, and document illicit money flows. The authors outline the challenges that law enforcement authorities which have already adopted AI-based investigative tools are facing, pointing out the need for a comprehensive legal framework for the development and use of AI specifically for law enforcement. In addition, they tackle the need for multi- and interdisciplinary research and knowledge sharing to achieve this.

Next, *Salomé Lannier* also looks at AI and law enforcement but with a focus on the fight against human trafficking. Lannier exposes a neglected area of research concerning the export and replication of AI systems for the detection and investigation of human trafficking schemes in the EU. She outlines the challenges that the use of these AI systems by European law enforcement authorities poses to European criminal national sovereignty and digital sovereignty, as these systems have primarily been developed and deployed by the USA and therefore embody specific U.S. values and policies.

In another article, *Randall Stephenson* and *Johanna Rinceanu* study the limitations of contemporary online regulatory frameworks by integrating insights from medicine and theoretical biology. They point out three reasons why contemporary Internet regulation is problematic: the lack of attention to the unique structural characteristics of today's digital media ecology; the desire to hastily and excessively harmonise online regulation, including the lack of sensitivity about the political and constitutional contexts called for by differences in human rights protection and constitutional structure; and the business models and economic motivations of digital platforms that lead to collateral censorship.

In the last article on AI, *Marcin Górski* considers the question of the use and possible replacement of a human judge by an AI judge. He argues that, while the use of AI instead of a judge would benefit the efficiency and predictability of the administration of justice, the use of AI judges would fall short in terms of independence, impartiality, and especially the fair trail principle.

This issue also explores topics going beyond the topical focus of AI but dealing with current issues that have triggered heated debate. Under the perspective of European law, *Oliver Landwehr* and *Erasmus Khan* reflect on the challenges of a possible cannabis legalization, arguing that the current prohibition regime has failed; the authors appeal for an interpretation of EU law that would allow for responsible regulation. *Laura Neumann,* for her part, provides guidance on the conditions that secondary EU legislation must fulfil in order to qualify as a legitimate legal basis for a limitation of the transnational ne bis in idem principle. She comes to similar results as the Advocate General in his recently released Opinion in the Volkswagen diesel emission scandal case (C-27/22 – see also news section, p. 35–36). Last but not least, *Jeffrey Simser* comments on recent Canadian court decisions regarding non-conviction based forfeiture in organised crime cases against motorcycle gangs.

Dr. Anna Pingen, eucrim editor

"Error 404 – Match not found"

Tax Enforcement and Law Enforcement in the EU Artificial Intelligence Act

David Hadwick

In EU Member States, tax administrations are the public organs that make most use of artificial intelligence (AI) and machine learning (ML) systems to perform State prerogatives. At least 18 EU Member States frequently use AI tax enforcement systems. In certain areas of taxation, such as value-added tax, AI and ML are already used throughout the EU. These systems perform a relatively broad range of tasks, reflecting the wide array of prerogatives of the administration itself. Generally, these different systems can be categorized into two archetypes: coercive and non-coercive AI systems. While non-coercive AI tax systems do not generate significant risks of conflict with taxpayers' fundamental rights, coercive AI tax systems used for tax enforcement bring about serious risks of conflict with taxpayers' fundamental rights and tax procedure as a whole. These risks have already materialised in a number of cases and have even led to serious scandals, such as *RoboDebt* and the *toeslagenaffaire*.

Yet, substantial confusion exists around the treatment of AI tax enforcement systems in the upcoming Regulation laying down harmonised rules on artificial intelligence ('EU AI Act') and whether these systems will be qualified as high-risk. Recital 38 of the current draft prescribes that systems used by tax administrations specifically for administrative purposes should not be viewed as high-risk AI law enforcement systems. While *prima facie* logical, distinguishing between administrative and law enforcement purposes is bound to be an impractical and arbitrary exercise. Law enforcement is becoming increasingly integrated through the involvement of administrative authorities and private actors, precisely because of the use of AI. In such contexts, the boundaries between administrative and penal processes are blurred and will generate confusion. By remaining attached to that anachronistic distinction, Recital 38 not only replicates that confusion but will exacerbate its effects.

I. Why AI Tax Enforcement Systems Are "High-Risk" Systems

In EU Member States, tax administrations are the public organs that make most use of artificial intelligence (AI) and machine learning (ML) systems to perform State prerogatives. Publicly-available data alone reveals at least 70 AI systems leveraged by national tax administrations, unequally spread over 18 EU Member States.[1] Even the EU itself, through Eurofisc members, has developed its own ML model: Transaction Network Analysis – a data matching model meant to detect missing trader intra-Community fraud.[2] Accordingly, in certain areas of taxation AI and ML are already used throughout the EU for the enforcement of taxation rules.

These AI tax enforcement systems perform a relatively broad range of tasks, reflecting the wide array of prerogatives of the administration itself. Generally, these different systems can be categorised into two archetypes. Some AI systems are leveraged by EU tax administrations for **non-coercive purposes,** including chatbots[3], nudging systems[4], and jurisprudence analysis[5]. These non-coercive systems constitute a minority of the models used by tax administrations in the EU, albeit a significant one.[6] The remainder AI systems are leveraged for **coercive purposes,** i.e. for tax enforcement tasks such as web scraping[7], the detection of statistical risk indicators[8,9], and risk scoring to screen and select taxpayers for audit.[10] In a little more than a decade, predictive analysis has radically transformed tax enforcement and tax administrations in the EU. Currently, the use of statistics and ML underpins all coercive prerogatives when selecting a taxpayer for audit. Data is collected and processed through ML and taxpayers are algorithmically selected on the basis of risk indicators inferred from ML predictions. The transformative power of AI is also reflected in the human resources of tax administrations, increasingly composed of data scientists and increasingly less of tax law experts.[11]

Some of these models were used by tax administrations in the EU as far back as 2004. This is for instance the case of XENON, a web scraping model leveraged by the Dutch tax administration *(Belastingdienst)*.[12] This means that tax administrations were pioneering public algorithmic governance long before debates over other popular buzzwords in predictive policing, such as facial recognition, biometric surveillance, social scoring, etc. The primary reason for the prominence of the use of AI systems by tax administrations is the immense documentary burden placed on tax offi-

cials. Each year, tax administrations must process billions of documents[13], answer millions of queries, and spend several millions of minutes on the phone.[14] Processing such volumes of data manually with the human resources of national tax administrations is simply impossible. Accordingly, long before the advent of AI, tax administrations were already using traditional statistical approaches and heuristics to perform their fiscal prerogatives. The transition from traditional statistics to automated statistics and machine learning did thus not constitute a major scale-up.

1. The risks of AI tax enforcement systems

The EU AI Act follows a risk-based approach, meant to strike a proportional balance between the two policy goals of the instrument, namely: the promotion of innovation and the protection of citizens fundamental rights. Accordingly, the Regulation outlines four levels of risk ranging from prohibited to minimal risk. Minimal risk systems (level 1) generally escape the scope of the instrument aside from the invitation to self-regulation through codes of conduct and limited risk systems (level 2) are only bound to minimum transparency requirements in specific use cases, particularly chatbots and deep fakes. Models deemed as bearing unacceptable risk (level 4) are prohibited. By sheer number of articles, the majority of obligations in the instrument are imposed on high-risk systems (level 3). According to the current draft proposal, organisations with high-risk systems must comply with strict requirements such as certification, data governance, transparency, human oversight, record-keeping and cybersecurity. Comparatively to the other levels of risk, the obligations imposed on high-risk systems are numerous and substantively detailed, often requiring granular control of specific externalities. Hence, the risk-based approach seeks to ensure that obligations imposed on an AI system are proportional to the risks it generates.

In that regard, AI tax enforcement systems should be viewed as "high-risk" because these systems have been shown to contain various sources of conflict with EU citizens' rights, documented in jurisprudence and doctrine. This is less true for **non-coercive AI tax systems,** in fact, some of these models are truly a net plus both for the administration and for taxpayers. Chatbots, for example, enable taxpayers to request information from the administration at any time of the day and year. Processing little to no taxpayer personal data[15],these systems have opened up a new channel of communication with tax officials, while alleviating the substantial administrative burden of tax officials. Reports indicate that chatbots reduce the number of queries directly sent to the administration by a margin of up to 90%, with very high satisfaction rates amongst taxpayers.[16] The same can be said of nudging, simply by adapting the language of default letters sent to taxpayers, e.g. referring to a taxpayer by his or her first name or by adding references to the benevolent purpose of tax collection, the speed and rate of compliance increase in noteworthy ways.[17]

Conversely**, coercive AI tax systems** used for tax enforcement bring about serious risk of conflict with taxpayers' fundamental rights and tax procedure as a whole. These risks have already materialised in a number of cases. Coercive AI systems can conflict with the principle of legality because they disrupt procedures to such an extent that these no longer reflect procedural codes. For instance in *eKasa*[18], the Slovak Constitutional Court ruled that machine-learning bolstered surveillance to such an extent that it required a specific framework and tailored safeguards to negate the risks of abuses. Currently, the majority of tax administrations in the EU use coercive AI systems without a specific legal basis to that effect and without safeguards to negate demonstrated risks of such systems.[19] This is problematic in terms of legality as the different externalities these systems generate cannot be systematically captured by existing procedural rules.[20] Most notably, these systems entail risks of conflict with the right to a private life and right to data protection, as seen for example in *SyRI*[21] or the State Council *(Conseil d'Etat)* on the use of web scraping[22]. The primary source of friction lies in the fact that tax administrations have adopted tools that increase their surveillance capability based on procedural rules that pre-date the internet. Through web scraping, tax administrations are capable of surveilling the internet, e-commerce platforms, social media, or satellite images without differentiation between compliant and non-compliant taxpayers. As these data processing activities are generally regarded as an administrative process, tax officials do not have to secure any form of prosecutorial assent to use web scraping systems and collect taxpayer personal data.[23] These tools collect bulks of data and match the data to the different taxpayers at a speed unrivaled by any human tax official, drastically increasing the scope of data collected and number of taxpayers surveilled by the administration. In spite of the apparent interferences with privacy, the use of web scraping by tax administrations in the EU, the scope of data collected, the sources of data collection, the limits and safeguards, etc. remain largely unregulated.[24]

Moreover, predictive models such as risk detection and risk scoring tools are prone to errors, statistical biases and discrimination. These models are *predictive,* hence these systems only forecast a *probable* outcome based on what is statistically likely. Such a process by nature involves a great deal of uncertainty, errors, and deviations from objective reality. For these reasons, predictive models have already resulted in serious scandals such as *Robodebt*[25] in

Australia and the *toeslagenaffaire*[26] in the Netherlands. The latter is perhaps the best illustration of the devastating consequences that AI tax enforcement systems may occasion, particularly when these are not sufficiently regulated.

2. The *toeslagenaffaire,* stark example of the risks of AI tax enforcement

In the *toeslagenaffaire*, the Dutch tax administration *(Belastingdienst)* attempted to automate the assessment of childcare allowance *(kinderopvangtoeslag)* fraud with a predictive model. The model had the power to, without any human input, discontinue the allowances of welfare recipients and request the reimbursement of all aids ever received. Parents labelled as fraudsters by the AI system were made to pay back large sums of money (€35,000 on average – up to €250,000), testimony to the high childcare costs in the Netherlands, among the highest in the OECD.[27] As the label was disclosed to other public and private actors, following so-called "linkage of records"[28], parents were denied credit cards, bank accounts, loans, other means of public assistance, etc. In some cases, child protective services paid visits to their children's school or homes to forcibly separate them from their parents.[29] Later inquiries by the State Secretary revealed that the predictions of the models were erroneous in 94% of cases.[30] A substantial part of these errors were the result of discrimination induced by the historical biases in data of the administration, data inaccuracies, and the processing of data on nationality and ethnicity by the risk scoring model.[31] A central element of the scandal was the fact that the model contained a feature "Dutch/non-Dutch" *(Nederlander/niet-Nederlander)* whereby the predicted risk of fraud of non-Dutch individuals was systematically increased. The application of such a model meant that foreign residents and dual nationals would be excessively targeted by the model, and thus disproportionately became the victim of unlawful reimbursement requests. Upon revelation of the scandal, the entire Dutch cabinet resigned. Estimations suggest that the cost may be totaling €5.5 billion in compensation for the estimated 40,000 victims.[32] Although the affair was revealed more than two and a half years ago, over 1,500 children have not yet been returned to their parents[33], and testimonies suggest that compensations could last until the year 2030.[34] The scandal perfectly illustrates the potential risks of AI tax enforcement to data protection, privacy, non-discrimination, fair trial, and good governance. The models of the tax administration target a wide and highly heterogeneous population, often based on inaccurate data sources[35], using opaque and potentially biased features. Leveraging statistics to profile taxpayers under such conditions significantly increases the risk of disparity and discrimination.

II. AI Tax Enforcement Systems and the Notion of "Law Enforcement" in the EU AI Act

Despite widespread use and empirically demonstrated risks, substantial confusion remains around the treatment of AI tax enforcement systems in the upcoming EU AI Act. Tax enforcement systems are conspicuously absent from the draft proposal despite AI tax enforcement systems having given rise to the most unsettling case of automation bias to date. The notion that such systems would not constitute a priority in an instrument meant to regulate the externalities of AI is astonishing. Yet, unlike justice, education or law enforcement, tax enforcement is not singled out as a specific area in Annex III of the proposal, where sectors with high-risk systems are listed. The absence of AI tax enforcement from the draft raises questions, particularly as the initial proposal was published in April 2021, a couple of months after the revelations around the *toeslagenaffaire*. To be qualified as high-risk, the only alternative is thus for tax enforcement systems to be allocated to another category listed in Annex III. By elimination, law enforcement appears as the likeliest candidate given that tax enforcement is, in part at least, a form of law enforcement. Tax officials enforce taxation rules, investigate tax crimes, and are viewed as a competent authority in the Law Enforcement Directive (LED).[36] However, Recital 37 of the Preamble of the initial draft proposal specified that AI systems used by tax administrations should not be regarded as systems used for the purpose of law enforcement. In a move completely at odds with the lessons learned in *toeslagenaffaire,* the draft proposal seemed to create an exemption for tax administrations whereby AI tax enforcement systems would not be regarded as high-risk. This position was striking as it was in direct conflict with the LED, of which the AI Act will be *lex specialis.*[37] The proposal was later amended by the common position of the Council.[38] Recital 38 (formerly 37) now prescribes that AI systems specifically intended for administrative purposes should not be regarded as high-risk systems used by law enforcement, establishing a strict dichotomy between AI used either for administrative or law enforcement purposes. A *prima facie* distinction between criminal and administrative processes seems to make sense under a risk-based approach. Crimes typically result in harsher sentences compared to administrative offences. In the Recital, the severity of sanctions for criminal offences is explicitly mentioned as a factor that should be taken into account. Yet, upon closer analysis, it appears that this dichotomy will generate additional confusion around the treatment of AI tax enforcement systems and whether these qualify as high-risk systems.

In the context of taxation, distinguishing between administrative and criminal offences is a complex and arbitrary

exercise. Rare exceptions aside, what distinguishes administrative from criminal offences in taxation is the subjective intention of the perpetrator. Simply put, a tax crime is a fiscal administrative offence committed intentionally. Hence, the salient feature is the *mens rea*. However, AI tax enforcement systems are not used to predicting the subjective intention of a perpetrator. These tools merely predict a risk of non-compliance based on objective material factors. This risk is forecast by examining the gradient between what is declared by a taxpayer, and what level of wealth is stochastically and comparatively probable. In other words, AI tax enforcement systems detect *actus reus,* not *mens rea.* As a result, AI tax enforcement systems are all used *interchangeably* both for administrative and criminal tax offences, none are used *specifically* for administrative purposes. Predictive policing tools of the tax administration are exclusively used in the audit phase, when subjective intentions have not yet been determined. Taxpayers are subjected to the same AI tax enforcement scrutiny whether they are subsequently suspected of fraud or cleared of any suspicion. The fact that the AI system is used to detect what is later qualified as an administrative or criminal offence has little bearings on the model itself and the risks resulting from its use. By the time the offence has been qualified, the model has generated all its potential risks. Yet, the obligations imposed on high-risk systems in the EU AI Act are not retroactive; in fact, most of these are pre-emptive and should be performed prior to using the model. In such a context, it is hard to see how the dichotomy of Recital 38 could be correctly applied. Furthermore, the definitions of fiscal crimes have not been harmonised in the EU, hence some offences may be of administrative nature in one Member State, while being a crime in another.[39] Based on the *Engel*[40] criteria, the dichotomy would rest primarily on the national law qualification of the offence, and whether it is viewed as a crime or an administrative offence in the respective jurisdiction. Since that qualification has not been harmonised, two identical tools may be categorised differently under the AI Act.

Seemingly, Recital 38 attempts to uphold a binary and obsolete notion of "law enforcement" in an era where policing is increasingly integrated. Law enforcement is an organic process involving a multitude of stakeholders, including the traditional police, administrative authorities, and even external corporate actors. This is particularly true for tax administrations that must, by virtue of the wide array of prerogatives performed, involve numerous public and private actors. Tax evasion and tax fraud are umbrella terms meant to qualify an enormous number of offences. Importing an excessive amount of cigarettes or liquor, illegal species of fauna and flora, counterfeited goods, not declaring workers, employing migrant workers, under-valuing an asset, and hiding financial assets are all considered forms of tax evasion and fraud. To detect these offences, the tax administrations continuously collaborate with other agencies, such as food safety administrations, asylum authorities, financial administrations, labour inspectorates, corporate brands, etc. In such a context, distinguishing between different actors and whether their role was incremental to administrative or punitive aspects of a procedure, is so complex that it is bound to be arbitrary. Tax enforcement is becoming increasingly integrated, precisely because of the integration of AI, as the use of certain models relies on the know-how of specific stakeholders. Corporations provide support to police forces and tax administrations, online, in public spaces, through proprietary models, etc.[41] NGOs and investigative journalists use web scraping to detect fraudulent schemes and tax evaders using offshore entities.[42] These actors are neither administrative nor criminal, yet play an integral role in the law enforcement apparatus.

III. Conclusion

Overall, the treatment of AI tax enforcement systems in the upcoming EU AI Act is riddled with uncertainty and confusion. Despite several amendments to the draft proposal, Recital 38 seems to raise more questions than it provides answers. Distinguishing between administrative and criminal processes is bound to be an arbitrary, impractical, and reductionist exercise. Moreover, given the state of harmonisation of fiscal crimes in the EU, a literal application of Recital 38 is likely to result in the fragmentation of EU law. While AI is upending pre-existing notions of tax enforcement and law enforcement as reflected in tax and criminal codes, EU legislators remain attached to an anachronistic vestige of public law. As such, this dichotomy is not novel, with this issue also reflected in the GDPR and the LED.[43] Yet, by resting a crucial part of the EU AI Act on this very distinction, the AI Act not only replicates that confusion but strongly exacerbates its effects.

The treatment of AI tax enforcement systems reveals a certain arbitrariness inherent to the risk-based approach in the EU AI Act. Discussions on the potential inclusion of ChatGPT and generative AI as high-risk systems in the proposal[44] indicate that the risk-based approach is excessively focused on buzzwords and may not be the product of a consistent methodology. Conversely, despite the empirically demonstrated prejudicial effects of these systems, tax enforcement is not viewed as warranting its own risk category in Annex III. Factually, the AI systems used by tax administrations are quite unique and do not always correspond to traditional predictive policing. Tax administra-

tions perpetually oscillate between administrative and law enforcement in ways that are hard to capture in a binary legal construct. This is perhaps indicative of AI tax enforcement systems requiring their own *sui generis* category with specific rules and limits, different from "law enforcement" as intended in the instrument. With its wide array of AI systems, both coercive and non-coercive, it is clear that AI tax enforcement escapes traditional dichotomies and legal qualifications. Attempting to fit tax enforcement within a pre-existing mold may thus not be the best strategy. The uniquely ambivalent nature of the tax administration and diversity of AI systems should warrant a dedicated sectorial instrument or specific area of attention in Annex III of the AI Act. In that regard, a risk-based approach should distinguish between non-coercive AI tax systems and coercive systems as suggested in this article.

David Hadwick
Doctoral researcher at the Centre of Excellence DigiTax, University of Antwerp, Belgium – PhD Fellow of the Research Foundation for Flanders (FWO)

1 D. Hadwick, "Behind the One-Way-Mirror: Reviewing the Legality of EU Tax Algorithmic Governance", (2022) 31(4) *EC Tax Review,* 1, 18. – for a complete breakdown of all the ML systems identified, see: D. Hadwick "AI Tax Admin EU" <https://www.uantwerpen.be/en/projects/aitax/country-reports/> accessed 4 April 2023.
2 OECD, Tax Administration Series: Comparative information on OECD and Other Advanced and Emerging Countries, 2021, p. 110; U. Turksen, Countering Tax Crimes in the European Union: Benchmarking the OECD's Ten Global Principles, 2021, p. 244; T. Wahl, "New Data Mining Tool to Combat Vat Fraud", *eucrim:* <https://eucrim.eu/news/new-data-mining-tool-combat-vat-fraud/> accessed 4 April 2023.
3 OECD, *Tax Administration Series: Comparative Information on OECD and other Advanced and Emerging Economies,* 2019, pp. 175–181.
4 M. Luts & M. Van Roy, "Nudging in the Context of Taxation – How the Belgian FPS Finance Uses Behavioural Insights to Encourage Taxpayers to Pay Faster" (2019) *IOTA Papers,* p. 7; D. van Hout, "Gedragsbeïnvloeding in het belastingrecht: Are you 'nudge'" (2019) *Tijdschrift voor Fiscaal Recht,* p. 928–936.
5 OECD Forum on Tax Administration (FAT), "Inventory of Tax Technology Initiatives", Table TRM1: <https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/tax-rule-management-and-application.htm> accessed 4 April 2023.
6 Web-scraping, Risk-detection and risk-scoring tools are significantly more prevalent in the EU (65% – 46 out of 70 models are coercive).
7 Décret n° 2021-2148 du 11 février 2021, Art. 4, III, 1°-2°.
8 OECD, *Advanced Analytics for Better Tax Administration* (2016), p. 23.
9 C. Williams, "Developing efficient risk assessment tools to tackle undeclared work: a toolkit" (2021), pp. 17–19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3944128> accessed 4 April 2023.
10 OECD, *Tax Administration Series: Comparative Information on OECD and other Advanced and Emerging Economies,* (2019), p. 52.
11 Dutch tax administration, Vacatures – out of 70 starter positions, 36 are IT and data analytics, while 20 are fiscal and juridical services: < https://werken.belastingdienst.nl/vacatures/starter/fiscaal-juridisch?order_by=publication_date> accessed 5 April 2021.
12 European Commission DG Taxation and Customs Union, Risk Management Guide for Tax Administrations – Fiscalis Risk Analysis Project Group (February 2006), p. 67.
13 Report from the EC to the Council and the EP COM (2017) 780 final, Eighth report under Article 12 of Regulation (EEC, Euratom) n° 1553/89 on VAT collection and control procedures, p. 11.
14 Dutch Tax Administration, *Belastingdienst* "10 miljoen telefoontjes aan de Belastingtelefoon in 2021' <https://over-ons.belastingdienst.nl/organisatie/feiten-en-cijfers/10-miljoen-telefoontjes-aan-de-belastingtelefoon-in-2021/> accessed 4 April 2023.
15 In fact, chatbots such as "steuerchatbot" in Germany advise taxpayers not to input any personal data, see: <https://steuerchatbot.digital-bw.de/steuerbw.html> accessed 4 April 2021.
16 OECD, *Tax Administration Series: Comparative Information on OECD and other Advanced and Emerging Economies, op. cit.* (n. 3).
17 M. Luts & M. Van Roy, (2019) *IOTA Papers*, *op. cit.* (n. 4); D. van Hout, (2019) *Tijdschrift voor Fiscaal Recht, op. cit.* (n. 4).
18 Constitutional Court of the Slovak Republic PL. ÚS 25 / 2019-117 (*eKasa* case).
19 OECD, *Tax Administration Series: Comparative information on OECD and Other Advanced and Emerging Countries, op. cit.* (n. 2).
20 For instance, the German Tax Code dates from 1919, see: K.-D. Drüen, "Tax in History: Hundred Years Tax Code in Germany", (2019) 47(11) *Intertax*, pp. 979–985.
21 Rechtbank Den Haag, 5 Februari 2020 – ECLI:NL:RBDHA:2020:1878 (*SyRI* case).
22 Cour Constitutionnelle, Décision n° 2019-796 du 27 décembre 2019 sur la loi de finances pour 2020, §§79–96 ; Commission Nationale Informatique & Libertés (CNIL), Déliberations n° 2019-114 du 12 Septembre 2019 portant avis sur le projet d'article 9 du projet de loi de finances pour 2020.
23 D. Dierickx, "The Belgian compliance model and methodology to obtain data from 'Sharing Economy' platforms" in: *IOTA* (ed.) *Disruptive Business Models – Challenges for Tax Administrations* (2017), pp. 21–23.
24 With the exception of Décret n° 2021-2148 du 11 février 2021, Art. 4, III, 1°-2° in France, *op. cit.* (n. 7), no procedural rules regulate the specific use of web scraping by tax administrations.
25 Court settlement *Robodebt* case: Federal Court of Australia, 23 Dec. 2020, *Prygodicz v. Commonwealth,* Order no. VID1252/2019.
26 Autoriteit Persoonsgegevens [Dutch Data Protection Authority], Belastingdienst/Toeslagen – De verwerking van de nationaliteit van aanvragers van kinderopvantoeslag, Rapport no. z2018-22445 (2020); Tweede Kamer der Staten-Generaal [Netherlands 2nd Parliamentary Chamber], Eindverslag Parlementaire ondervragingscomissie Kinderopvantoeslag "Ongekend Onrecht", pp. 3–7 (The Hague, 17 Dec. 2020).
27 S. Ranchordás, & L. Scarcella, "Automated Government for Vulnerable Citizens: Intermediating Rights" (2021). *30(2) William & Mary Bill of Rights Journal,* 373–418.
28 Dutch Ministry of Justice (Ministerie van Justitie en Veiligheid), "Nota naar aanleiding van het verslag inzake de Tijdelijke wet

uitwisseling persoonsgegevens UHP KOT" (11 January 2023), pp. 2–4.
29 L. Kok, "Kabinet: Mogelijk meer dan 1115 kinderen in toeslagenaffaire gedwongen uit huis geplaatst", *AD*, 21 October 2021: <https://www.ad.nl/politiek/kabinet-mogelijk-meer-dan-1115-kinderen-in-toeslagenaffaire-gedwongen-uit-huis-geplaatst~ad7a83e4/> accessed 4 April 2023.
30 Tweede Kamer der Staten-Generaal, Eindverslag "Ongekend Onrecht", *op. cit.* (n. 26), pp. 22–23.
31 See Autoriteit Persoonsgegevens, *op. cit.* (n. 26).
32 J. Frederik, "De compensatieregeling voor de toeslagenaffaire is een fiasco van 5,5 miljard. Wat nu?", *De Correspondent,* 2 February 2022: <https://decorrespondent.nl/13097/de-compensatieregeling-voor-de-toeslagenaffaire-is-een-fiasco-van-5-5-miljard-wat-nu/787932533003-ef601d9e> accessed 4 April 2023.
33 See Autoriteit Persoonsgegevens, *op. cit.* (n. 26).
34 I. de Kruif, "Compensation ouders toeslagenaffaire kan zomaar tot 2030 duren", *NOS*, 18 January 2023: <https://nos.nl/nieuwsuur/artikel/2460354-compensatie-ouders-toeslagenaffaire-kan-zomaar-tot-2030-duren> accessed 4 April 2023.
35 E.g. data collected on social media platforms or data emanating from denunciations made by other taxpayers.
36 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union legislative acts, COM(2021) 206 final.
37 Art. 2 & Art. 3(7), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.* 119, 4.5.2016, 89.
38 Council of the European Union 'General approach' to Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union legislative acts, 25 November 2022, Interinstitutional File: 2021/0106 (COD), 38.
39 J. Cremers, "EU Company Law, Artificial Corporate Entities and Social Policy" (2019) *European Trade Union Confederation*, 36.
40 ECtHR, 23 November 1976, *Engel and others v Netherlands*, Appl. no. 5100/71 et al., para 82.
41 B. Kennedy and L. Ryder, *IBM Public Safety Solutions for a Safer Planet,* 2021, pp. 5–7.
42 A. Palionis, "Web Scraping for Transparency", *New Digital Age*, 30 September 2022: <https://newdigitalage.co/?s=Web+Scraping+for+Transparency> accessed 4 April 2023.
43 CJEU Case C-175/20, 24 February 2022, *SIA ‚SS' v Valsts ieņēmumu dienests,* para 35 to 42.
44 G. Volpicelli, "ChatGPT broke the EU plan to regulate AI", *Politico*, 3 March 2023: <https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/> accessed 5 April 2023.

Artificial Intelligence in Law Enforcement Settings

AI Solutions for Disrupting Illicit Money Flows*

Athina Sachoulidou, Dimitrios Kafteranis, and Umut Turksen

With the rise and spread of ICT-enabled crimes and illicit money flows (IMFs), law enforcement authorities and financial intelligence units need innovative investigative tools and skills, and organisational and regulatory adjustments to counter crime. The multi-disciplinary TRACE project is developing AI solutions to identify, track, and document IMFs to pave the way for effectively prosecuting money laundering and predicate offences and recovering criminal proceeds. In this article, the authors present the TRACE project to reveal some of the challenges faced by law enforcement authorities in adopting AI-driven investigative tools, taking into account the ongoing legislative procedures in preparation for the adoption of the EU Artificial Intelligence Act. It is argued that more empirical research is required on the design and feasibility of these AI-enabled tools given their implications for various legal principles, such as privacy, data protection, and the right to a fair trial. An "ethics and rule of law by design" approach, as is also being pursued by the TRACE project, is mapped out as a robust framework for developing AI tools intended to be used for law enforcement purposes.

I. Introduction

Rooted in popular culture, the catchphrase "follow the money" is often invoked in the context of investigations aimed at uncovering financial malfeasance.[1] As Europol notes: "To effectively disrupt and deter criminals involved in serious and organised crime, law enforcement authorities need to follow the money trail as a regular part of their criminal investigation with the objective of seizing criminal profits".[2]

This is particularly true for investigating money laundering, which involves disguising the proceeds of criminal activity (predicate offences) to make them appear legitimate. By following the money trail, namely identifying individuals, companies, or transactions that require closer scrutiny, law enforcement authorities (LEAs) are able to seize criminal assets and profits, and bring offenders to justice.[3]

The European Union (EU) and its Member States are not immune from cross-border financial crime, including but not limited to money laundering. To address this phenomenon, the EU has taken various legislative measures and is currently negotiating a new anti-money laundering and countering the financing of terrorism legislative package that was first proposed in July 2021.[4] The creation of the European Public Prosecutor's Office (EPPO) consolidated the EU's institutional framework in this regard.[5] While it is also putting in place steps towards a more efficient legal framework for combatting financial crime, the development of new technologies has opened up new opportunities for criminals to exploit in many different areas, such as crypto-assets and fast internet connections.[6] Notwithstanding the above, such technologies may also revolutionise the way LEAs gather and evaluate evidence in order to assist criminal justice authorities in prosecuting crime effectively, particularly to the extent that borderless crime requires cross-border cooperation.

Combining expertise in computer engineering, law, and social sciences from academia, policy makers, and law enforcement agencies, the TRACE project has embarked on exploring illicit money flows (IMFs) in the context of six use cases: terrorist financing, web forensics, cyber extortion, use of cryptocurrency in property market transactions, money laundering in arts and antiquities, and online gambling.[7] Its ultimate goal is to equip European LEAs with the tools and resources necessary to identify, track, document, and disrupt IMFs in a timely and effective manner. This can involve, among other things, the analysis and visualisation of financial data (virtually in any given language), the identification of suspicious financial activity patterns, and collaboration with other agencies to share information. These tools are developed with the help of cutting-edge technologies, such as artificial intelligence (AI) and machine learning (ML). As a consequence, they should represent trustworthy solutions adhering to the rule of law, fundamental rights, and ethical design principles. For this purpose, the TRACE project has a dedicated work package (WP8) on the ethical, legal, and social impact of the AI solutions it develops.[8]

Informed by the research conducted for the TRACE project, this article outlines some of the key findings on the use of AI in law enforcement settings as follows: Firstly, it provides a conceptual framework, including a definition of AI (Section II). Secondly, it explains how AI systems may reshape law enforcement with an emphasis on crime analytics (Section III), and which law governs such uses of AI (Section IV). In doing so, the article employs EU law as a system of reference and sheds light on the AI governance model included in the European Commission's Proposal for a Regulation laying down harmonised rules on AI (EU AIA).[9] Finally, by critically analysing the EU legal regime for AI, the article identifies key shortcomings and offers suggestions and recommendations (Section V).

II. Conceptual Framework: Definition of AI and Data Informing AI Systems

Although there is (still) no unanimously accepted definition of AI,[10] the past two decades have been marked by the exponential development of AI systems using algorithms, statistical models, and other techniques. These are used to analyse and interpret large amounts of data (originating from various sources and often referred to as "big data"), with the help of advances in computing power, and to make predictions or decisions based on the analysis of this data.[11] This goes hand in hand with the diversification of AI applications, including natural language processing, image and voice recognition, autonomous vehicles, and predictive analytics.

At policy-making level, as early as in 2018, the UK government referred to AI in its Industrial Strategy White Paper as: "[t]echnologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition and language translation".[12] In the same year, the European Commission, in its Communication on AI for Europe, emphasised not only the element of intelligent behaviour, but also the degree of autonomy AI systems may present.[13] Furthermore, the Commission set up a multi-disciplinary expert group, namely the High-Level Expert Group on AI (AI HLEG) to clarify the definition of AI and to develop ethics guidelines for trustworthy AI.[14] The findings of this group have informed the first attempt to regulate AI at EU level, i.e. the EU AIA, which includes a proposal for the first formal legal definition of AI. In particular, Art. 3 nr.1 EU AIA defines an "AI system" as: "software that […] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[15] Designed to classify AI as a sociotechnical concept, this definition has also been used by the TRACE project.

AI applications are data-driven applications. The data used to train an AI system, and the data it processes, depend on the type of tasks a system is designed to perform. AI systems intended to be employed for law enforcement purposes are no exception, namely they require various types of data, whether personal[16] or not, to become effective. This may include, for instance: 1) data on past criminal activity that can be used to train AI systems to forecast criminal activity, 2) social media data that can be analysed to identify behavioural patterns that correlate with suspicious activity, 3) demographic data, such as age, gender, race, that can be used to inform decisions about the allocation of law enforcement resources, or 4) travel, communication, and financial data, the combination of which can decode the specifics of past criminal activity.

Gathering and processing data for developing, training, and using AI systems may raise significant ethical and legal issues, including but not limited to privacy, data protection, bias, and due process.[17] To capitalise on the benefits of data-driven applications in a law enforcement environment, it is therefore imperative that the respective algorithms are trained and supplied with *accurate* data, previously collected in appropriate contexts, and that this data is properly linked, in order to avoid false negatives and, more importantly, false positives.[18] What is more, the data used to train an algorithm may reflect discriminatory practices and entrench biases.[19] One danger of algorithmic bias is the generation of a bias "feedback loop", in which the analysis or predictions of an ML-based system influence how the same system is validated and updated.[20] In other words, this is a case of algorithms influencing algorithms, because their analysis then influences the way LEAs act on the ground.[21] If the algorithmic output were to be used in law enforcement decisions or even as evidence in a courtroom, this reality could adversely affect the rights of the defence and lead to severe consequences, including deprivation of a person's freedom.[22] This suggests that high-quality and accurate data is needed to ensure that the resulting predictions, decisions, or actions are also accurate, fair, and unbiased. In fact, the respective AI systems should be tested and audited for accuracy and fairness on a regular basis.[23]

III. Use of AI in Law Enforcement Settings

The use of AI for law enforcement purposes has already been challenged by legal scholars with the focus placed predominantly on predictive policing and facial recognition, that allows for the automatic identification or authentication of individuals, and on AI applications employed in criminal proceedings to calculate the risk of recidivism.[24]

The EU AIA covers the use of AI in law enforcement settings in two scenarios. Firstly, it prohibits the use of real-time remote biometric identification systems in publicly accessibly spaces unless this is strictly necessary for achieving the purposes set out in Art. 5 (1) lit. d.[25] Secondly, the EU AIA classifies other AI systems employed for law enforcement purposes as high-risk (Art. 6) – based on the risks they may pose to fundamental rights (recital 38) – and stipulates a series of legal obligations on their providers (see Section IV). In particular, point 6 Annex III to EU AIA introduces a typology of high-risk automated law enforcement, including AI systems intended to be used:

- For individual risk assessments of natural persons in order to assess the risk of (re-)offending or the risk for potential victims of criminal offences (lit. a);
- As polygraphs and similar tools or to detect the emotional state of a natural person (lit. b);
- To detect deep fakes (lit. c);
- To evaluate the reliability of evidence in the course of criminal investigations or crime prosecution (lit. d);
- For predicting the (re-)occurrence of an actual or potential crime based on profiling of natural persons (Art. 3 (4) Directive (EU) 2016/680) or assessing personality traits and characteristics or past criminal behaviour of natural persons and groups (lit. e);
- For profiling of natural persons in the course of crime detection, investigation or prosecution (lit. f);
- For crime analytics regarding natural persons, allowing LEAs to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data (lit. g).

This typology does not include AI-driven consumer products that may not be intended for law enforcement purposes but do have the potential to produce an output of probative value that could be evaluated as a piece of evidence before criminal courts.[26]

In the context of AI-driven crime analytics, AI can be used to organise, categorise, analyse, and interpret suspicious activity reports and evidence and, in particular, electronic evidence (such as online shopping, financial transactions, emails, chat logs, social media posts, and the corresponding subscriber and traffic data) with the aim of consolidating the prosecution files. This suggests that the respective evidence, corresponding to *past* criminal activity, has already been collected, with or without the help of AI applications. In that sense, the focus lies on identifying patterns in the data available to LEAs and connections that may not be visible to human analysts or the detection of which may be particularly resource- and time-consuming.[27]

The TRACE tools, which are aimed at disrupting IMFs that usually comprise voluminous, often publicly accessible data, fit better into the category of AI-supported crime analytics (point 6, lit. g EU AIA), considering that their current design does not allow for individual risk assessment or for profiling of specific natural persons. Based on this classification, the TRACE consortium has decided to comply with the requirements set out in arts. 6–52 EU AIA. Interestingly, however, all Compromise Texts released to date and the Council's General Approach to the EU AIA do not list AI-supported crime analytics anymore under high-risk AI systems and, thus exempt the providers of those systems from complying with the requirements for developing high-risk AI.[28]

IV. What Law – if any – Governs AI Systems in Law Enforcement Settings?

Currently, there is no specific law in the EU that governs the use of AI in law enforcement settings. However, there are several existing legal frameworks that may apply to the development and use of AI in general and AI-driven crime analytics in particular.

1. Data protection and management

The rights to privacy and to personal data protection (arts. 8 European Convention on Human Rights (ECHR); 7–8 Charter of Fundamental Rights of the EU (CFR)) are cardinal with respect to both the development and the use of AI applications. Out of the EU laws setting out data protection and management rules, the focus lies on Regulation (EU) 2016/679 (a.k.a. GDPR), and Directive (EU) 2016/680,[29] known as LED. The envisaged TRACE tool, which is intended to assist LEAs in investigating IMFs by, *inter alia,* visualising nodes and edges in real-life scenarios of money laundering and various predicate offences, cannot fully exclude access to and processing of personal data, even if publicly accessible data is given priority.

For data protection purposes, it is important to distinguish the stage of *developing* AI-driven crime analytics tools, which is governed by the GDPR, from that of LEAs *applying* such tools for operational purposes. The latter is governed by the LED to the extent that processing of personal data takes place. The LED – whilst having the same axiological basis as the GDPR, presents different nuances as to, for instance, enforceable data subject rights or the powers of data protection authorities related to the particularities of the police and criminal justice environment (see recitals 10, 11).[30] This means that personal data has to be processed lawfully for law enforcement purposes and that such personal data processing is also governed by the principles of purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality (Art. 4 (1) LED). However, similar to data subject rights, these principles have been adapted to ensure a certain level of flexibility, in order to accommodate special security-related needs and day-to-day law enforcement practices.[31]

When it comes to the lawfulness of personal data processing for law enforcement purposes, the LED is more restrictive compared to the GDPR and its legal bases for personal data processing (Art. 6 GDPR). More specifically, Art. 8 (1) LED states that:

> Member States *shall* (emphasis added) provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) [namely prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security] and that it is based on Union or Member State law.

The processing of personal data is therefore only legal if it is linked to a task within the Directive's scope, as specified in the domestic laws transposing it.[32]

Art. 9 LED is applicable in the testing phase of AI-driven applications, when LEAs use LEA datasets that are only available to them. This dictates that personal data collected by competent authorities for the purpose of the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal sanctions may only be processed for other purposes, *if such processing is authorised by Union or Member State law. I*n this case, the GDPR is applicable, unless the processing is carried out as part of an activity which falls outside the scope of Union law (Art. 9 (1) LED). The GDPR is also applicable when LEAs process personal data for, *inter alia*, scientific purposes (Art. 9 (2) LED).

Furthermore, LEAs, in their capacity as data controllers, are obliged to conduct a data protection impact assessment (DPIA) as required by Art. 27 (1) LED "where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons". At a minimum, the DPIA must contain: a general description of the envisaged processing operations; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged to address those risks; safeguards; security measures; and mechanisms to ensure the protection of personal data and to demonstrate compliance with the LED (Art. 27 (2) LED). Importantly, the LED's wording makes a DPIA mandatory when it comes to the use of new technologies for personal

data processing in a law enforcement environment.[33] This suggests that the future use of TRACE tools on the part of national LEAs will require a DPIA.

Finally, gathering and processing non-personal data is governed by Regulation (EU) 2018/1807,[34] which "aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users" (Art. 1). Data localisation requirements may be imposed on grounds of public security (including crime investigation, detection, and prosecution) in compliance with the principle of proportionality (Art. 4 (1)). Recital 9 expressly refers to AI as one of the major sources of non-personal data – with aggregate and anonymised datasets used for big data analytics being a specific example of non-personal data. Should it become possible to turn anonymised data into personal data, such data is to be treated as personal, and the GDPR applies accordingly.

2. Protection of fundamental rights

When AI is employed in fields tightly linked to public governance, such as law enforcement, it is necessary to broaden the scope of human rights considerations, namely to go beyond privacy and data protection as part of the ethical and legal impact assessment of the respective applications.[35] In other words, one should take a holistic approach to the protection of human rights of the affected individuals.[36] This also includes *procedural* fundamental rights, considering that, for instance, AI-driven crime analytics aims at organising and evaluating information of probative value for crime prosecution purposes. Thus, the legal framework that governs the utilisation of AI in law enforcement settings should comprise the ECHR and the CFR, complemented – with respect to defence rights – by EU secondary laws.[37]

In addition, the EU AIA adopts a risk-based approach to AI systems on the basis of their implications for safety, health, and fundamental rights (recitals 13, 27–28). This also applies to AI systems intended to be used for law enforcement purposes, which are classified as high-risk, considering the power imbalance inherent in law enforcement, the risk of discrimination and unfair treatment associated with the lack of high-quality data, accuracy, robustness *as well as* the risk of hampering important procedural fundamental rights that arises from a lack of transparency, explainability, and documentation (recital 38). As such, automated law enforcement applications must comply with certain requirements before they can be placed on the market or used in the EU. In particular, these requirements include the establishment, implementation, documentation, and maintenance of a risk management system (Art. 9), the use of high-quality training, validation, and testing datasets (Art. 10), technical documentation that enables the assessment of the AI system's compliance with the requirements set out in the EU AIA (Art. 11), logging capabilities (Art. 12), design enabling the interpretability of the system (Art. 13), and safeguarding human oversight (Art. 14), accuracy, robustness, cybersecurity (Art. 15).[38] These are significant safeguards to ensure that AI systems used in law enforcement do not perpetuate biases or discriminate against certain individuals or groups, are transparent and fair, and do not cause harm. In that sense, these requirements represent an important step towards ensuring that automated law enforcement applications are used responsibly and ethically.

V. Areas of Contention and Reform

The planned decategorisation of AI-driven crime analytics as high-risk, as part of the ongoing negotiations on the EU AIA, may be aligned with the realities of police investigations in the digital age, but remains predominantly effectiveness-centred. This approach fails to pay heed to the risks and challenges arising from the data-intensive character of these applications,[39] the potential bias inherent in the training and validation datasets as well as in the data which the system processes, or the risks inherent in repurposing AI and, particularly, the inadvertent shift from pattern-based to individual-based data mining. Additionally, it does not take into account the numerous societal concerns regarding the automation of law enforcement – concerns primarily related to risks to citizens' rights, ranging from privacy and non-discrimination to the fair trial principle – emerging from the use of unchecked or not sufficiently checked AI by LEAs. Such concerns suggest that the exceptions suggested by the Council's Compromise Texts and General Approach to the EU AIA should be treated with caution and require clear checks and balances.

Another area of regulation that requires further scrutiny when it comes to the specificities of using AI in law enforcement settings is the adoption of design standards at the EU level in order to ensure the responsible and ethical use of such AI applications in the future. The design frameworks for such standards and regulations must be informed by ethics, the rule of law, and fundamental rights.[40] This presupposes the cooperation between multiple stakeholders, including technology experts and end-users, policy- and law-makers, civil society, and affected individuals. Indeed, one of the unique features of TRACE Project is that scholars with legal, social, and ethical background are working closely with technical partners, LEAs and an independent ethics advisory board in an open dialogue so as to under-

stand and provide solutions to all the relevant issues raised by AI tools. This multidisciplinary and collaborative style of research should be encouraged for the development of AI tools. The TRACE tripartite methodology of fundamental rights sensitive design[41] can serve as a reference for the future development of AI tools for law enforcement purposes.

VI. Conclusion

AI tools have the potential to assist investigators in analysing large amounts of data quickly and accurately, allowing them to identify patterns and insights that may be significantly more difficult to discern manually. With these upsides also come downsides– revealing, thus, the need for regulation. While there are various legal instruments which could be applied to AI in law enforcement, it is essential to have a comprehensive legal framework for the development *and* use of AI systems in general, and for law enforcement specifically. To that end, further multi- and interdisciplinary research and knowledge exchange are required. The TRACE Project is a good example of this approach, which is desirable not only for the development of AI tools in compliance with the rule of law and fundamental rights, but also for instilling societal trust in AI.

* Research for this article is part of the TRACE Project (https://trace-illicit-money-flows.eu) which received funding from the EU Horizon 2020 Research & Innovation Programme under Grant Agreement No. 101022004.

1 The expression "follow the money" was popularised by the 1976 film "All the President's Men" that depicted the investigation into the Watergate scandal. It is used to refer to the tracing of financial transactions in order to unveil criminal activity.

2 Europol, "Enterprising criminals: Europe's fight against the global networks of financial and economic crime", 2021, p. 4 <https://www.europol.europa.eu/publications-events/publications/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime> accessed 4 April 2023.

3 P. Alldridge, "Criminal asset recovery and the pursuit of justice", (2018) 21(1) *Journal of Money Laundering Control*, 16–32.

4 For an overview of the scheduled amendments of the EU AML/CFT legal framework see <https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en> accessed 4 April 2023.

5 Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("the EPPO").

6 See Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2021" <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021> accessed 4 April 2023.

7 See TRACE blog posts at <https://trace-illicit-money-flows.eu/news/> accessed 4 April 2023.

8 For more information, see <https://trace-illicit-money-flows.eu/project-outcomes/> accessed 4 April 2023.

9 European Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", COM (2021) 206 final, Art. 3 (1).

10 For detailed definitions and applications of AI, see U. Turksen, "Legal and Societal Impacts of Lethal Autonomous Weapons Systems (LAWS)" in: A. Aigner, H. Cremer-Schäfer and A. Pilgram (eds.), *Gesellschaft. Kritik. Ironie: Liber Amicorum für Reinhard Kreissl*, 2023, pp.167–196; J.D. Joseph and U. Turksen, "Harnessing AI for Due Diligence in CBI Programmes: Legal and Ethical Challenges", (2022) 4 (2) *Journal of Ethics and Legal Technologies*, 3–25.

11 T. Wischmeyer and T. Rademacher (eds.), *Regulating Artificial Intelligence*, 2020, paras. 5–6.

12 Department for Business, Energy and Industrial Strategy, "Industrial Strategy: Building a Britain for the future" <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf/> accessed 4 April 2023, p. 37.

13 Communication from the Commission, "Artificial Intelligence for Europe", COM/2018/237 final, p. 1.

14 See AI HLEG, "A definition of AI: Main capabilities and disciplines. Definition developed for the purpose of AI HLEG's deliverables" (2019) <https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf/> accessed 4 April 2023; *id*, "Ethics Guidelines for Trustworthy AI" (2019) <https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai/> accessed 4 April 2023.

15 Following the adoption of the Council's common position (general approach) on the EU AIA, the definition of the term "AI system"

Athina Sachoulidou, Dr.
Assistant Professor in Criminal Law, Centre for Research on Law and Society (CEDIS), NOVA School of Law, Universidade Nova de Lisboa

Dimitrios Kafteranis, Dr.
Assistant Professor in Law, Centre for Financial and Corporate Integrity (CFCI), Coventry University

Umut Turksen, Dr.
Professor in Law, Centre for Financial and Corporate Integrity (CFCI), Coventry University

reads: "a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts".

16 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 1.

17 N. Geslevich Packin and Y. Lev-Aretz, "Learning algorithms and discrimination", in: W. Barfield and U. Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence*, 2018, pp. 88–94.

18 See S. Greenstein, "Preserving the rule of law in the era of artificial intelligence (AI)" (2022) 30 *Artificial Intelligence and Law*, 291–323; A. Sachoulidou, "Going beyond the 'common suspects': to be presumed innocent in the era of algorithms, big data and artificial intelligence" (2023) *Artificial Intelligence and Law*, <https://link.springer.com/article/10.1007/s10506-023-09347-w#Sec4/> accessed 4 April 2023.

19 See, for instance, B.D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter and L. Floridi, "The ethics of algorithms: Mapping the debate" (2016) 3(2) *Big Data & Society*, 1–12.

20 See European Agency for Fundamental Rights (FRA), "Bias in Algorithms – Artificial Intelligence and Discrimination" (2022) <https://fra.europa.eu/en/publication/2022/bias-algorithm/> accessed 4 April 2023, pp.29–48.

21 Cf. M. Oswald, J. Grace, S. Urwin and G.C. Barnes, "Algorithmic risk assessment policing models: lessons from the Durham HART model and 'experimental' proportionality" (2018) 27(2) *Information & Communication Technologies Law*, 223–250.

22 See F. Palmiotto, "The black box on trial: The impact of algorithmic opacity on fair trial rights in criminal proceedings", in: M. Ebers and M. Cantero Gamito (eds.), *Algorithmic governance and governance of algorithms*, 2018, pp. 49–70; A. Sachoulidou, *op. cit.* (n. 18).

23 See European Parliament, "Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters", 2020/2021(INI) <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html/> accessed 4 April 2023.

24 See G.G. Fuster, "Artificial Intelligence and Law Enforcement. Im pact on Fundamental Rights" (2020), <https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2020)656295> accessed 4 April 2023.

25 These include the targeted search for specific potential victims of crime, the prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or of a terrorist attack, or the detection, localisation, identification, or prosecution of those involved in the offences listed in Art. 2 (2) of the Council Framework Decision 2002/584/JHA (European Arrest Warrant) and punishable with at least three years' imprisonment.

26 See S. Gless, "AI in the courtroom: a comparative analysis of machine evidence in criminal trials" (2020) 51(2) *Georgetown Journal of International Law*, 195–253.

27 Cf. European Police Chiefs, "Joint Declaration on the AI Act" (20 22), p. 1, <https://www.europol.europa.eu/cms/sites/default/files/documents/EPC%20Joint-Declaration%20on%20the%20AI%20Act.pdf/> accessed 4 April 2023.

28 Council, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text", 14278/21, <https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf/> accessed 4 April 2023; "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Second Presidency compromise text", 11124/22, <https://data.consilium.europa.eu/doc/document/ST-11124-2022-INIT/en/pdf/> accessed 4 April 2023; "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Presidency third compromise text (Articles 1–29, Annexes I–IV)" 12206/1/22, <https://data.consilium.europa.eu/doc/document/ST-12206-2022-REV-1/en/pdf/> accessed 4 April 2023; "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Fourth Presidency compromise text", 13102/22, <https://data.consilium.europa.eu/doc/document/ST-13102-2022-INIT/en/pdf/> accessed 4 April 2023; "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach (25 November 2022)", Interinstitutional file: 2021/0106 (COD) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> accessed 4 April 2023.

29 Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

30 See P. De Hert and V. Papakonstantinou, "The new Police and Criminal Justice Data Protection Directive" (2016) 7(1) *New Journal of European Criminal Law*, 7–19; J. Sajfert and T. Quintel, "Data Protection Directive (EU) 2016/680 for police and criminal justice authorities", in: M. Cole and F. Boehm (eds.) *GDPR Commentary*, 2018; L. Drechsler, "Comparing LED and GDPR Adequacy: One Standard Two Systems", (2020) 1(2) *Global Privacy Law Review*, 93–103.

31 De Hert and Papakonstantinou, *op. cit.* (n. 30), 9, 11–12.

32 T. Wischmeyer and T. Rademacher (eds.), *op. cit.* (n. 11).

33 N. Geslevich Packin and Y. Lev-Aretz, *op. cit.* (n. 17).

34 Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.

35 Cf. FRA, "Getting the future right – Artificial intelligence and fundamental rights" (2020), p. 7, <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights/> accessed 4 April 2023.

36 See A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, 2022, pp. 12–13.

37 See, for instance, Directive 2012/13/EU on the right to information in criminal proceedings; Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.

38 Cf. the changes undertaken in the formulations of the so-called essential requirements in Council, 'General Approach' *op. cit.* (n. 28).

39 Cf. A. Mantelero, *op. cit.* (n. 36), pp. 2–3.

40 See AI HLEG, *op. cit.* (n. 14), p. 21; K. Yeung, A. Howes and G. Pogrebna, "AI Governance by Human Rights–Centered Design, Deliberation, and Oversight: An End to Ethics Washing", in: M. Dubber, F. Pasquale and S. Das (eds.), *The Oxford Handbook of Ethics of AI*, 2020, pp. 76–106.

41 See E. Aizenberg and J. van den Hoven, "Designing for human rights in AI" (2020) *Big Data & Society*, 1–14.

Using US Artificial Intelligence to Fight Human Trafficking in Europe

Potential Impacts on European Sovereignties

Salomé Lannier

Human trafficking is keeping pace with new technologies, but so is its repression. Nowadays, artificial intelligence (AI) systems support the daily work of law enforcement authorities in detecting and investigating trafficking schemes. These systems were developed, and are used primarily, in the United States of America (US). As the fight against human trafficking is a worldwide priority, they are often exported from the US or replicated. Yet, so far, little research has been done to examine how (US) policies and values might be embedded in these specific systems. This article argues that the spread of US tools using artificial intelligence to combat human trafficking hinders the autonomy of foreign States. Particularly in the European context, these tools might challenge national criminal sovereignty as well as Europe's digital sovereignty. The article highlights the US policies surrounding human trafficking that are embedded in these AI systems (legal definition, political priorities and decisions) and the lack of adequate consideration of existing European standards. These are meant to protect human rights while developing and using AI systems, i.e. the protection of personal data and control over technical standards.

I. Introduction

In public international law, sovereignty derives from the independence and autonomy of States. The parallel aspect of enjoying the monopoly of legitimate authority over a territory is the exclusion of other States' authority.[1] At the core of the autonomy of States' sovereignty lies their criminal sovereignty: defining offences, sanctions, powers of investigation, policies, priorities, etc.[2] Yet, sovereignty was mainly conceptualised in the 16th century,[3] and such idealization of States' autonomy strikes us a utopia in our globalised[4] and digitalised[5] world. Consequently, the concept of digital sovereignty was developed to adapt to new realities. Originally meant as informational sovereignty (control over information[6]), today digital sovereignty covers different concepts, such as technological sovereignty and data sovereignty,[7] due to the lack of a uniform use. In this article, the modern-day theory of (digital) sovereignty will allow us to highlight the contradiction between the supposed autonomy of States and the "*de facto* disparities of power among States, which, in turn, might limit their capacity to act, to regulate and to freely adopt decisions."[8] These disparities of power are particularly threatening to independent sovereignty when they impact criminal law, which is seen as being at the heart of the State's monopoly of legitimate violence.[9]

One of these disparities of power lies in the ability to develop, to use, and to regulate artificial intelligence (AI) systems when applied to repress criminal offences. Since AI relies on humans and institutions for its creation and functioning, "it depends entirely on a […] set of political and social structures."[10] While no unique definition exists regarding AI,[11] computer systems have been assisting States' decision-making processes since the 1970s.[12]

There are many examples of AI systems in use to support the prevention and prosecution of offences. Human trafficking (in particular for the purpose of sexual exploitation) is taken as an example in this article to draw conclusion on the use of AI systems for law enforcement purposes, as they have received little attention from legal scholars (in this area) until now. Human trafficking is an internationally criminalised offence defined in the 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Art. 3.a). It is defined as follows:

> [t]he recruitment, transportation, transfer, harbouring or receipt of persons [element 1: actions], by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person [element 2: coercive means], for the purpose of exploitation [element 3: purpose].

Therefore, trafficking represents a security threat violating the human rights of victims. Protecting victims and prosecuting perpetrators is a manifestation of States' criminal sovereignty. Nowadays, the fight against human trafficking is also at the crossroads of States' digital sovereignty. Indeed, technologies, in particular the internet, can exac-

erbate the trafficking schemes. Consequently, the term e-trafficking was "coined to describe human trafficking facilitated/enabled or regulated through the use of the internet and other communication platforms."[13] To recruit victims, traffickers actively impersonate an employer, rely on cyber seduction,[14] or use different types of bait online, usually a false job offer.[15] The internet is used to book transportation and accommodation for the potential victim.[16] During the exploitation stage, when the victims are trafficked for the specific purpose of sexual exploitation, technology enables their sexual services to be advertised online.[17] Although trafficking encompasses many forms of exploitation (sexual exploitation, labour exploitation, forced begging and criminality, etc.), American AI systems exclusively, as far as we know, focus on the repression of the federal offence of "sex trafficking." Thus, the intended comprehensive approach of the human trafficking phenomena adopted by this article is limited by the existing technologies. Traffickers might take advantage of technology for the anonymity it provides or to hasten trafficking processes. However, e-trafficking also creates data that might be helpful to investigators and used as evidence. Yet, the sheer volume of data challenges their productive analysis by law enforcement authorities.

The creation of AI systems was intended as a solution, namely to support the fight against human trafficking facilitated by the internet. It can automate the crawling and processing of data, organise information linked to ongoing cases, or improve the detection of patterns and red flags to multiply proactive investigations. This idea was first developed by researchers in the United States in 2012.[18] Later, their elaboration was framed into the Defense Advanced Research Projects Agency.[19] Currently, similar systems are being developed outside of the US (e.g. in Canada[20]), and US systems are being exported to Europe (e.g. to the United Kingdom and to Ireland[21]). However, the actual or potential use of foreign tools, especially within the European Union, is not neutral with respect to the autonomy of European sovereignties. The following two sections analyse the risks inherent in the use of US AI systems to the criminal national sovereignty and the digital European sovereignty.

II. Risks of Influencing European *Criminal* Sovereignty

First, the spread of US AI systems developed to support the investigation and prosecution of sex trafficking questions the protection of European national criminal sovereignty. AI systems might be seen as neutral, as they are based on objective data and criteria to combat well-defined criminal phenomena. However, such a perspective reflects mere technological solutionism;[22] it "would postulate the existence of a technical solution to any problem."[23] However, these systems are actually not neutral, as they might be imbued with political positions and policies. As such, when they are used abroad, the politics of their State of origin might be applied in the States of reception, potentially impacting the latter's autonomous sovereign powers. This risk genuinely exists regarding AI systems designed to prevent and prosecute human trafficking.

Despite benefiting from an international definition, the offence of human trafficking has not been fully harmonised. Firstly, the 2000 Protocol was adapted and broadened by European texts[24] (the addition of types of exploitation and suppression of the criterion of a transnational traffic). Secondly, even within Europe, national definitions reveal a wide variety of transpositions of the Directive 2011/36/EU.[25] For instance, in Belgium, coercive means are not an element of the offence but an aggravating circumstance.[26] In France and in Spain, as in the supranational definitions, these means are part of the elements of the offence, although they are slightly differently defined.[27] A comparison between the European definitions and the US code is particularly striking; the latter only recognises trafficking in the context of, on the one hand, peonage, slavery, involuntary servitude, or forced labour, and, on the other hand, sex trafficking.[28] Therefore, an AI system to combat human trafficking needs to be adaptable to national definitions, which might not be applicable, as most of them were developed in the United States and for the United States.

The development of such systems is based on the criminal realities and priorities of each country, particularly regarding the types of exploitation. For instance, in Europe, there is a stronger focus on trafficking for labour exploitation.[29] Yet, systems of AI financed in the United States exclusively focus on the repression of trafficking for domestic sexual exploitation.[30] One of the major means is the analysis of classified advertisements. In particular, these US AI systems emphasise the identification of victims who are minors.[31] The fact that the existing systems are mainly made in the United States impacts worldwide priorities in the fight against the complex and multifaceted phenomenon of human trafficking. It reinforces the continuous focus on sexual exploitation,[32] which has been strongly criticised as a very limited conception of human trafficking.[33]

In the latter context, one should consider as well that trafficking for sexual exploitation can, under some national legislations, be conflated with sex work. Certain states' policies consider commercial sex as exploitative *per se*, regardless of working conditions and the legitimacy of a sex workers' agency.[34] This is the case in the United States, where sex

work is mainly illegal.[35] On the contrary, there are various sex work regulations in Europe: legal regulation (the Netherlands, Germany), prohibition (Romania), criminalisation of clients (France, following the Nordic model)[36], and decriminalization (Belgium[37]). To qualify as an act of adult sex trafficking in the United States, the US code only requires a commercial sexual act as the purpose. Yet, it still requires proof of "means of force, threats of force, fraud, [or] coercion"[38] (child trafficking does not require this element: to identify an underage trafficked victim, an AI system would only have to detect underage persons advertised for a commercial sexual act). Nevertheless, indicators of potential trafficking in advertisements for sex workers' services hardly take this element into consideration; they rely only on indirect potential flags of exploitation[39] (it is obviously rare to find explicit proof of coercion in the ads). They have been identified on the basis of US prosecutions and by experts and databases, but the indicators remain the basis of the criteria used abroad, although criminal realities might differ.[40] It must be pointed out that American researchers developing these systems mostly rely on a conflation between trafficking and sex work, and they do not consider nor mention the existing discussions on whether sex trafficking should be, or not, conflated with sex work.[41] Researchers and sex workers have come to criticise the criteria set by the systems as not being able to detect victims of trafficking but instead discriminating sex workers.[42] Consequently, this conflation is embedded in the functioning of most of the US systems of AI designed to support the investigation of sex trafficking cases. Therefore, their use in Europe, in particular in countries where sex work policies are different, could have a significant impact on the autonomy of their criminal sovereignty.

III. Risks of Influencing European *Digital* Sovereignty

Apart from the potential threat to European criminal national sovereignty by not taking into account national definitions, law enforcement priorities, and the delimitation of human trafficking, the use of AI systems originating from the United States to prevent and combat human trafficking in Europe might also hinder digital sovereignty.

Firstly, the use of AI systems from the United States challenges data sovereignty, which is understood as "the ability to store and process certain types of data."[43] Classical sovereignty prioritises the possibilities to exercise control and authority over data. Interpreted through the lens of human rights, sovereignty also includes the protection of citizens' personal data. Data, in particular personal data, is a "genuine power issue between States."[44] EU data sovereignty, in particular, lies in its innovative and unique approach to protect it. Processing personal data for the purpose of combating an offence is regulated by Directive 2016/680.[45] Despite setting out more lenient obligations than the General Data Protection Regulation,[46] the Directive still lists a number of principles to be implemented by design (Art. 4), which can be summarised as the following:

- Lawful and fair processing, delimited by specific purposes;
- Limitation of collection and conservation of data;
- Data accuracy, integrity, and confidentiality;
- Liability on the part of the data processor.

If AI systems have been developed in the United States for an originally American-only use, however, these AI systems do not fall within the scope of the European data protection framework. Therefore, it is doubtful whether the protection of personal data has been incorporated into the systems from the start of their development. Since the transparency principle is absent from the Directive, the necessary safeguards to control the use of these AI systems are particularly important to balance any interference with the right of privacy.

Another important point is the localisation of the processed data. Indeed, it would be particularly sensitive to store European data related to criminal investigations in the United States if the AI systems use a cloud version saved on US servers. The Directive provides for the possibilities of transferring data outside the EU (Arts. 35 to 40). Specifically, the Umbrella agreement was signed between the EU and the United States on this matter in 2016.[47] A few months earlier, the Privacy Shield[48] set a supposedly adequate level of data protection for data transfers for commercial and civil purposes. Yet, it was invalidated by the CJEU.[49] On the contrary, the lawfulness of the Umbrella agreement has not been questioned. As these AI systems process large quantities of data, including, sensitive data, the effectivity of safeguards when data is transferred abroad should be particularly reviewed.

Secondly, European digital sovereignty is not limited to data sovereignty but also covers the regulation of technical aspects, leading to a technical sovereignty. Indeed, Directive 2016/680 hardly considers the specificities of AI systems. For instance, it does not take into account the principle of transparency or the explanation of the algorithms that comprise the AI system,[50] even though this is at the core of ensuring that data used to train it does not lead to any discrimination.[51] The Directive also does not take into consideration any protection against discriminating results.[52] This is why the European Commission launched a proposal for an AI Act in 2021.[53] This act would apply whenever the AI systems are used by European users, including law en-

forcement authorities (Art. 2.2). As these systems are to be used for the prosecution of offences (Art. 7.1.a in relation to Annex III.6), they are classified as high-risk and must comply with the highest level of obligations. Yet, transparency obligations have been excluded for these systems (Art. 52).

While this act is still under negotiation, the CJEU provided guidance for the regulation of automated systems. In its Opinion of 2017 on the EU-Canada PNR Agreement, the Court recognised the possibility of carrying out an automated analysis based on predefined models and criteria and a comparison with various databases.[54] The Court introduced five elements to assess the lawfulness of the use of AI systems to prosecute offences:[55]

- Establishing specific, reliable, and non-discriminatory models and criteria to ensure the targeting of individuals with a level of "reasonable suspicion";
- Using automated means only for serious transnational crime;
- Ensuring databases are reliable and up-to-date;
- Introducing an individual re-examination by non-automated means to offset the margin of error;
- Concluding a review of the implementation.

Against this background, it should be stressed that the US systems are mainly used to assist in the investigation of domestic trafficking, which calls into question their applicability in Europe. The conclusion on data sovereignty applies to technical sovereignty: US systems did not integrate European standards (existing standards and those under development) when developing their algorithm. Furthermore, when the software code is developed by private entities, the lack of transparency and the protection of the code by intellectual property rights challenge the access to technical elements to ensure their conformity to European frameworks.

IV. Conclusion

As human trafficking schemes are being increasingly supported by online services, one challenge for law enforcement to combat human trafficking lies in the processing and organisation of available data online. It is next to impossible for individual investigators to develop an efficient means of manually processing data. Manual processing is indeed unsuitable for the volume of data and to keep up with the speed of deletion and updates. As a solution, the automatic processing of data and systems relying on AI have been developed to assist law enforcement authorities. These instruments are intended to support the exercise of sovereignty by states by protecting their populations and borders.

Yet, AI systems used to combat offences are not neutral: depending on the context of their development, they embed specific values and policies. As such, due to the digital interconnectedness of the world, if exported abroad, they might hinder the autonomy of other States by limiting their own exercise of sovereign powers.

A first challenge in this regard relates to European *criminal* national sovereignty In particular as regards human trafficking, systems are based on a specific national definition of an offence that might not be consistent with foreign definitions. Similarly, they are often developed in a particular national criminal context, making them harder to adapt to foreign criminal realities if a consistent reprogramming is not considered. Furthermore, because they were developed primarily in the United States, they underline a continued focus on combating sex trafficking while disregarding other forms of trafficking, such as labour exploitation. Lastly, the American AI systems have usually been programmed according to a prohibitionist policy that equates sex trafficking with sex work, which leads to these values and political decisions being integrated in the systems. All of these elements indicate that the autonomy of European national criminal justice sovereignty could be threatened if American systems are used or if national systems are developed on the basis of American systems without specific adaptation.

The use of US AI systems in Europe to combat human trafficking also challenges European *digital* sovereignty. The EU has developed regulations and standards to safeguard the protection of personal data and the specific risks linked to the use of AI systems. Yet, these norms are not applicable to systems originally developed for a US-only use. Although transparency requirements of AI systems are to be limited when used by law enforcement authorities, European norms under development still require conformity with human rights standards. This reinforces the potential threats to European autonomy when developing AI systems that are consistent with its own policies and values, both from a criminal law and a human rights perspective.

1 K. Irion, "Government Cloud Computing and National Data Sovereignty", (2012) 4(3–4) *Policy & Internet*, 40, 53.
2 M. Massé, "La souveraineté pénale", (1999) *Revue de science criminelle et de droit pénal comparé*, 905, 905.
3 J. Bodin, J.H. Franklin, *On sovereignty: four chapters from the six books of the commonwealth*, Cambridge University Press, Cambridge texts in the history of political thought, 1992.
4 J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018.
5 M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020.

Salomé Lannier
PhD candidate, University of Bordeaux (France) and University of Valencia (Spain)

6 A. Gotlieb, C. Dalfen, K. Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", (1974) 68(2) *American Journal of International Law*, 226.
7 Communication from the Commission, "Shaping Europe's digital future", COM(2020) 67 final, p. 2.
8 T. Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", (2020) *SSRN Scholarly Paper, ID 3748098*, <https://papers.ssrn.com/abstract=3748098> accessed 28 February 2023.
9 M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004.
10 K. Crawford, *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021, 8.
11 One definition is the following: a "set of scientific methods, theories and techniques whose aim is to reproduce, by a machine, the cognitive abilities of human beings", European Commission for the Efficiency of Justice (Council of Europe), "European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment", 2018, 69.
12 D.K. Citron, "Technological Due Process", (2008) 85(6) *Washington University Law Review*, 1248, 1257.
13 S. Milivojević, "Gendered exploitation in the digital border crossing? An analysis of the human trafficking and information-technology nexus", in: M. Segrave and L. Vitis (eds.), *Gender, Technology and Violence*, 2017, pp. 28–29.
14 Resolution 27/2 of the Commission on Crime Prevention and Criminal Justice, Economic and Social Council, United Nations, "Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies", E/2018/30 E/CN.15/2018/15.
15 L. Holmes, "Introduction: the issue of human trafficking", in: L. Holmes (ed.), *Trafficking and human rights: European and Asia-Pacific perspectives*, 2010, pp. 1, 9; Council of Europe report by A. Sykiotou, "Trafficking in human beings: Internet recruitment – Misuse of the Internet for the recruitment of victims of trafficking in human beings", 2007, p. 32; A. Lavorgna, *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*, Thesis, University of Trento, 2013, p. 126; A. Di Nicola, G. Baratto, E. Martini, *Surf and sound – The role of the internet in people smuggling and human trafficking*, University of Trento, ECrime Research Reports, 2017, p. 62.
16 Europol Intelligence Notification 15/2014, "Trafficking in human beings and the internet", 2014.
17 J. Middleton, "From the Street Corner to the Digital World: How the Digital Age Impacts Sex Trafficking Detection and Data Collection", in: J. Winterdyk and J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, 2020, pp. 467, 471; J.L. Musto, D. Boyd, "The Trafficking-Technology Nexus" (2014) 21(3) *Social Politics*, 461, 467; B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures – Quelles réalités sociales et juridiques?*, Rapport de recherche, Université de Bordeaux, CNRS – COMPTRASEC UMR 5114, 2020, p. 45.
18 E. Kennedy, *Predictive Patterns of Sex Trafficking Online*, Thesis, Carnegie Mellon University, 2012.
19 P. Szekely et al., "Building and Using a Knowledge Graph to Combat Human Trafficking", in: M. Arenas et al. (eds.), *The Semantic Web – ISWC 2015: 14th International Semantic Web Conference, Bethlehem, PA, USA, October 11–15, 2015, Proceedings, Part II*, 2015, p. 205; C. Pellerin, "DARPA Program Helps to Fight Human Trafficking", *U.S. Department of Defense*, <https://www.defense.gov/News/News-Stories/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/> accessed 28 February 2023; Department of Justice of the United States of America, "National Strategy to Combat Human Trafficking", 2017, p. 11.
20 Mila, "Infrared: AI for combating human trafficking in Canada", *Mila*, <https://mila.quebec/en/project/ai-for-combating-human-trafficking-in-canada/> accessed 28 February 2023.
21 Marinus Analytics, "About", *Marinus Analytics*, <https://www.marinusanalytics.com/about> accessed 4 October 2022.
22 E. Morozov, *To save everything, click here: the folly of technological solutionism*, 1st ed. PublicAffairs, 2013.
23 Y. Meneceur, *L'intelligence artificielle en procès: Plaidoyer pour une réglementation internationale et européenne*, Bruylant, 2020, p. 2; M. Broussard, *Artificial unintelligence: how computers misunderstand the world*, The MIT Press, 2018, pp. 7–8.
24 Council of Europe Convention n°197 on Action against Trafficking in Human Beings, 2005; Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, *O.J.* L 101, 15.4.2011, 1.
25 S. Lannier, "Le blanchiment d'argent dans le cadre de la traite d'êtres humains en sa forme d'exploitation sexuelle : une approche comparative", Master Dissertation, University of Bordeaux and Vietnam National University, 2019, pp. 32ff. Case law also highlighted the potential multiple interpretations of the concept, L. Esser, C. Dettmeijer-Vermeulen, "The Prominent Role of National Judges in Interpreting the International Definition of Human Trafficking" (2016) 6 *Anti-Trafficking Review*, 91; E. Coreno, "Finding the Line between Choice and Coercion: An Analysis of Massachusetts's Attempt to Define Sex Trafficking" (2021) 13(1) *Northeastern University Law Review*, 124.
26 Articles 433 quinquies and 433 septies of the Belgium criminal code.
27 Article 225-4-1 of the French criminal code; article 177 bis of the Spanish criminal code.
28 18 U.S. Code § 1590 and § 1591.
29 Group of Experts on Action against Trafficking in Human Beings (Council of Europe), "Guidance note on preventing and combatting trafficking in human beings for the purpose of labour exploitation", GRETA(2020)12; Communication from the Commission, "EU Strategy on Combatting Trafficking in Human Beings 2021–2025", COM(2021) 171 final, pp. 7–8.
30 Yet, most of the titles of the articles on them are misleading, as they target human trafficking in general; see, for instance, M. Ibanez, D. Suthers, "Detection of Domestic Human Trafficking Indicators and Movement Trends Using Content Available on Open Internet Sources", (2014) *47th Hawaii International Conference on System Sciences*, <http://ieeexplore.ieee.org/document/6758797/> accessed 28 February 2023; A. Dubrawski et al., "Leveraging Publicly Available Data to Discern Patterns of Human-Trafficking Activity" (2015) 1(1) *Journal of Human Trafficking*, 65; P. Szekely et al., *op. cit.* (n. 19), p. 205.
31 B. Westlake, M. Bouchard, R. Frank, "Comparing Methods for Detecting Child Exploitation Content Online", (2012) *European Intelligence and Security Informatics Conference*, <http://ieeexplore.ieee.org/document/6298826/> accessed 28 February 2023, 156; H. Wang et al., "Data integration from open internet sources to com-

bat sex trafficking of minors" (2012) *Proceedings of the 13th Annual International Conference on Digital Government Research*, <http://dl.acm.org/citation.cfm?doid=2307729.2307769> accessed 28 February 2023; D. Roe-Sepowitz et al., *Online Advertisement Truth Set Sex Trafficking Matrix: A tool to Detect Minors in Online Advertisements*, Research Brief, Arizona State University School of Social Work, Office of Sex Trafficking Intervention Research (STIR), 2018.

32 Only two European researchers tried to develop systems applied to job advertisements, with limited success: R. McAlister, "Webscraping as an Investigation Tool to Identify Potential Human Trafficking Operations in Romania", (2015) *Proceedings of the ACM Web Science Conference on ZZZ – WebSci'15*, <http://dl.acm.org/citation.cfm?doid=2786451.2786510> accessed 28 February 2023; A. Volodko, E. Cockbain, B. Kleinberg, "'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers" (2020) 23 *Trends in Organized Crime*, 7.

33 J. Chuang, "Giving as Governance? Philanthrocapitalism and Modern-Day Slavery Abolitionism", (2015) 62 *UCLA Law Review*, 1522.

34 J.E. Halley et al., "From the International to the Local Feminist Legal Responses to Rape, Prostitution/Sex Work and Sex Trafficking: Four Studies in Contemporary Governance Feminism", (2006) 29(2) *Harvard Women's Law Journal*, 347; C. Plumauzille, "Prostitution", in: J. Rennes (ed.), *Encyclopédie critique du genre*, 2021, p. 590.

35 R. Russo, "Online Sex Trafficking Hysteria: Flawed Policies, Ignored Human Rights, and Censorship" (2020) 68(2) *Cleveland State Law Review*, 314, 323.

36 S.Ø. Jahnsen, H. Wagenaar (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, 1st ed., 2019.

37 Loi modifiant le Code pénal en ce qui concerne le droit pénal sexuel, 2022.

38 18 U.S. Code § 1591(a).

39 Setting aside criteria linked to minority: shared management, geographic displacements, E. Kennedy, *op. cit.* (n. 18); shared phone number, M. Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Center on Communication Leadership & Policy, University of Southern California, 2012; inconsistencies in story, third party language, ethnicity, potential restricted movement ("in calls only"), M. Ibanez, D. Suthers, (2014) *47th Hawaii International Conference on System Sciences*, *op. cit.* (n. 28) 1556; unconventional sex advertised, disguised phone number, transient language, M. Hultgren, *An exploratory study of the indicators of trafficking in online female escort ads*, Thesis, San Diego State University, 2015. On the contrary, considering weak signals of coercion such as "*Physical injury, Subjected to violence, Timid, Forced to have sex, Women beaten*" in tweets, S. Andrews, B. Brewster, T. Day, "Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online" (2018) 7(1) *Security Informatics*, 3; and "*Impairment (vulnerability) Under the influence of drugs or alcohol, symptoms of mental illness or impairment*," D. Bounds et al., "Uncovering Indicators of Commercial Sexual Exploitation" (2020) 35(23–24) *Journal of Interpersonal Violence*, 5607.

40 B. Cartwright et al., *Deploying artificial intelligence to detect and respond to the use of digital technology by perpetrators of human trafficking*, International CyberCrime Research Centre – Simon Fraser University, 2022 ; L. Giommoni, R. Ikwu, "Identifying human trafficking indicators in the UK online sex market" (2021) *Trends in Organized Crime*, < https://doi.org/10.1007/s12117-021-09431-0> accessed 11 October 2022.

41 On the contrary, explicitly trying to differentiate between consensual sex work and sexual exploitation, refer to E. Simonson, *Semi-Supervised Classification of Social Media Posts: Identifying Sex-Industry Posts to Enable Better Support for Those Experiencing Sex-Trafficking*, Master thesis, Massachusetts Institute of Technology, 2021; B. Cartwright et al., *op. cit.* (n. 38).

42 R. Kjellgren, "Good Tech, Bad Tech: Policing Sex Trafficking with Big Data" (2022) 11(1) *International Journal for Crime, Justice and Social Democracy*, 149; M. Draughn, "No Ground Truth: Sex Trafficking and Machine Learning", *Windypundit* <https://windypundit.com/2022/07/no-ground-truth-sex-trafficking-and-machine-learning/> accessed 23 August 2022.

43 K. Irion, (2012) 4(3–4) *P&I*, *op. cit.* (n. 1), 40, 62.

44 M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 22.

45 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, *O.J.* L 119, 4.5.2016, 89.

46 In particular, regarding the principle of transparency, information, and obligations to delete, O. Tambou, J.F. López Aguilar, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, pp. 130–131, 188–194, 202.

47 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, *O.J.* L 336, 10.12.2016, 3.

48 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–U.S. Privacy Shield (notified under document C(2016) 4176), *O.J.* L 207, 1.8.2016, 1.

49 CJEU, 16 July 2020, Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*.

50 Commission White Paper, "Artificial Intelligence – A European approach to excellence and trust", COM/2020/65 final, p. 17.

51 European Union Agency for Fundamental Rights, "#BigData: discrimination in data supported decision making", 2018.

52 S. Wachter, B. Mittelstadt, L. Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7(2) *International Data Privacy Law*, 82.

53 Proposal from the Commission, "Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts", COM/2021/206 final.

54 CJEU, 26 July 2017, Opinion 1/15, *Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data*, para. 168.

55 *Ibid.* para. 172–174. Further criteria were developed when "it covers, generally and indiscriminately, the data of person s using electronic communication systems", CJEU, 6 October 2020, Joined Cases C-511/18, C-512/18, and C-520/18, *La Quadrature du Net, and Others*, para. 174–191.

Digital Iatrogenesis

Towards an Integrative Model of Internet Regulation

Randall Stephenson and Johanna Rinceanu

Limitations associated with online regulatory frameworks can be better understood by integrating pertinent insights from medicine and theoretical biology. Using insights from the biopsychosocial model, we argue that contemporary Internet regulations are problematic for three reasons. First, they pay insufficient attention to the unique structural characteristics of our digital media ecology, which raise significant epistemological concerns for online regulators. Second, differences in human rights protection and constitutional structure present further challenges requiring keen sensitivity to political and constitutional contexts for optimizing regulatory calibration. Third, our digital media landscape is dominated by private digital platforms whose unprecedented power and business models increasingly imperil the quality and quantity of public discourse, and facilitate privatization of government censorship under the rubric of human rights protection. Without carefully considering these structural differences, regulators – much like physicians – can too easily find themselves treating only symptoms rather than the underlying ailment.

I. Introduction

Synergies between the outwardly disparate disciplines of law and medicine can be observed well into our recent past. Addressing such affinities at a Harvard Law School lecture in 1895, the celebrated legal realist and later US Supreme Court Justice *Oliver Wendell Holmes Jr* proposed that "[a]n ideal system of law should draw its postulates and its legislative justification from science".[1] Years later, addressing members of the New York Academy of Medicine, Justice *Holmes*' successor and great admirer *Benjamin Cardozo*, then Chief Judge of the New York Court of Appeals, explored the significance of this interdisciplinarity in a memorable speech entitled "What Medicine Can Do For Law".[2] Along with his realist contemporaries who conceived of lawyers as "social clinicians" in a progressive era of "scientific jurisprudence",[3] *Cardozo* endorsed the growing scientific trend for "continuity of knowledge",[4] which challenged traditional academic subdivisions as largely false-to-facts and misleading.[5] Advocating for greater integration between the legal and medical sciences, *Cardozo* proposed that when searching for answers to problems of constitutional limitation or permissible encroachments on liberty, courts and legislatures should increasingly turn to "[…] medicine – to a Jenner or a Pasteur or a Virchow or a Lister as freely and submissively as to a Blackstone or a Coke".[6] Importantly, theirs was a time when felt necessities required physicians to concentrate on "individual" practices of diagnosis and prescription, while solutions to broader social problems were thought the sole purview of lawyers and politicians.[7] In an era of growing scientific rivalry between analytical research and intellectual synthesis, both Justices endorsed the latter by encouraging a multidimensional approach to scientific and legal fact finding, formulating value judgments, and charting effective political and legal reforms.

In today's digital media environment, any sustained course of intellectual isolationism is neither feasible nor desirable. As shown by the European Union's latest regulatory framework,[8] along with parallel North American developments aiming to remedy offensive online content,[9] there remains an urgent need for our medical and legal professions to join forces in seeking effective solutions to global Internet regulation by better understanding online social problems that have radically changed their epistemic nature and receptiveness to standard politico-legal interventions. Whether considering Europe's ascendant "notice-and-takedown" model, which relies upon and strengthens public/private co-optation – or the North American model of "market self-regulation", which immunizes digital intermediaries from liability for speech torts and provides greater protection for "offensive" speech – these models represent different approaches to regulating online communications, and symbolize profound disagreement on free speech's role and relationship to democratic governance.

In this article, we argue that contemporary Internet regulations are problematic for three reasons. First, they pay insufficient attention to the unique structural characteristics of our digital media ecology, which raise significant epistemological concerns for online regulators. Without carefully

considering these structural differences, regulators – much like physicians – can too easily find themselves treating only symptoms rather than underlying diseases and their aetiology. Second, differences in human rights protection and constitutional structure present further challenges, particularly in filtering and blocking online speech, which require keen sensitivity to political and constitutional contexts for optimizing regulatory calibration. Third, the unprecedented power of private digital platforms that own and effectively control the Internet's infrastructure facilitates privatized government censorship which, along with existing economic incentives, imperils the quality and quantity of public discourse.

Overall, we are confronting a unique regulatory dilemma involving the balancing of many "opposed maximisers", such as freedom of expression, social media platforms' interests in censoring and selling user content for profit, and the functional needs of deliberative democracy and holding power to account. To adapt a phrase popularized by philosopher and social critic *Ivan Illich,* any resulting imbalance in our online regulatory milieu can be fairly seen as lying at humanity's collective feet – a new, potentially more dangerous form of "digital iatrogenesis" is now upon us.[10]

II. Online Governance in Europe

Internet regulation is dominated in Europe by an emergent "notice-and-takedown" approach. Leading examples are Germany's pioneering Network Enforcement Act *(Netzwerkdurchsetzungsgesetz – NetzDG)*,[11] and the EU's new Digital Services Act (DSA).[12]

1. Germany's *NetzDG:* "notice-and-takedown" model

The world's principal Internet regulatory model is epitomized by Germany's *NetzDG*, which entered into force on 1 October 2017. Intending to improve upon digital intermediaries' efforts to address problematic online content by modifying their Terms of Use, *NetzDG* introduced a mandatory regulatory framework, which included severe penalties for non-compliance. From inception, *NetzDG* triggered controversy and widespread concern about its implications for freedom of speech and fundamental rights, both within and outside Germany.[13]

Employing a "notice-and-takedown" approach necessitating extensive public and private co-operation, *NetzDG* obliges digital media platforms to delete or block illegal online content within prescribed time periods ranging from 24 hours to seven days.[14] *NetzDG* defines "illegal content" by referencing numerous infractions in Germany's Criminal Code, including such reputational and public order offences as insult and disturbances to the public peace.[15] Digital platforms are obliged to inform complainants of their decisions and reasoning, and must indicate any rights of appeal.[16] Platforms are further obliged to report their content moderation activities on their websites and in the German Federal Gazette (*Bundesanzeiger*).[17] Notably, platforms are obliged to report potentially criminal content – including relevant IP addresses – to Germany's Federal Criminal Police Office (*Bundeskriminalamt*).[18] Online users will be notified no earlier than four weeks after this transmission. Penalties for non-compliance under *NetzDG* are harsh. Systematic non-compliance attracts fines of up to €50 million for corporate entities, and up to €5 million for corporate officials.

Germany's approach to regulating online communications has proven immensely popular, with over 25 countries and the EU having adopted or proposed legislation that directly or indirectly follows *NetzDG*'s example.[19]

2. EU's Digital Services Act: "notice-and-action" model

There is perhaps no greater evidence of *NetzDG*'s influence than recent enactment of the EU's DSA.[20] Designed as a cornerstone for shaping Europe's digital future, DSA aims to create a safe, predictable, and trustworthy online user environment.[21] In particular, DSA aims to "harmonize" online governance by countering harmful online content – particularly hate speech, disinformation, and other objectionable content – in a manner consistent with fundamental rights.

Directly applicable to all 27 EU Member States, DSA imposes on EU-based private digital intermediaries the primary responsibility for handling illegal online content.[22] Similar to *NetzDG*'s "notice-and-takedown" model, DSA introduces a "notice-and-action" mechanism that requires digital platforms to provide an accessible and user-friendly procedure by which users can complain about illegal online content. The pivotal aspect is the concept of "illegal content", which is defined in Art. 3(h) DSA as: "[…] any information that […] is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law". This definition is thus significantly broader than the German counterpart in § 1(3) *NetzDG*, which covers only violations of designated criminal provisions. Penalties for non-compliance can be significant, and are

indexed to platforms' size and their degree of impact on the public sphere.[23]

Complaints of "illegal content" can come from two sources – individuals or entities. Regardless of source, DSA requires platforms to respond in a timely, diligent, non-arbitrary and objective manner, notifying them of their decision and any possible legal remedies.[24] Notices submitted by "trusted flaggers" are given priority and processed on an expedited basis.[25] "Trusted flagger" status is granted under DSA to public or private entities (i.e. not individuals) with sufficient expertise and competence handling illegal content (e.g. Europol, INHOPE Association). Finally, a key component of the "notice-and-action" model is Art. 9 DSA, which requires platforms to comply with EU Member State orders to act against specific items of illegal online content.

DSA differs from *NetzDG* in several material respects. First, DSA decrees no specific period for content removal, requiring instead a "timely" decision, thereby allowing platforms additional flexibility to review challenged content. In fact, digital platforms are exempted from liability if they act "diligently" to delete or block access to illegal content or activities. Consistent with its aim of respecting fundamental rights, platforms must also explain to users any restrictions imposed and their legal or contractual basis.[26] Users can appeal platforms' content moderation decisions through internal complaint-handling mechanisms, out-of-court dispute settlement, or judicial redress.[27] Second, unlike *NetzDG*'s strict requirements, DSA requires platforms to notify authorities only when they are aware of information giving rise to a suspicion that a criminal offence involving a threat to life or personal safety has or is likely to occur.[28] Third, DSA does not oblige digital platforms to vigilantly monitor their website traffic for illegal content.[29]

In the end, by enacting DSA, the EU aims to not only guarantee a trustworthy online environment that effectively counters illegal online content, but to offer a regulatory "complete code". Consistent with this "harmonization" aim, DSA will supersede national regulations relating to matters falling within its scope.[30] In due course, Germany's *NetzDG* will accordingly give way to DSA's revised regulatory framework.

III. Online Governance in North America

Compared with the predominant "notice-and-takedown" model, the United States and Canada have adopted different approaches that highlight many of the emerging challenges of global Internet regulation.

1. United States of America's "market self-regulation" model

A further online regulatory model is "market self-regulation", which is canonically associated with the United States of America. This model represents a fundamentally different approach to regulating online content, and symbolizes deep disagreement on the constitutional role of freedom of expression in democratic nations.[31]

This model has two main elements. The first is that digital platforms are protected from civil liability for offensive speech acts under section 230 of the Communications and Decency Act (CDA).[32] Congress initially passed section 230 to protect online platforms from state liability for speech torts, the operative language being: "[n]o provider or user of an interactive computer service shall be treated as the *publisher* or *speaker* of any information provided by another information content provider".[33] American courts have since held that section 230 not only protects digital intermediaries against defamation liability, but more broadly against claims based on third-party content such as "[…] negligence; deceptive trade practices, unfair competition, and false advertising; the common-law privacy torts; tortious interference with contract or business relations; intentional infliction of emotional distress; and dozens of other legal doctrines".[34] According to leading Internet attorneys, this broad safe harbor represents "the cornerstone of a functioning Internet".[35]

The second element of the "market self-regulation" model is an enlarged scope of protection for offensive online speech – including hate speech – under the First Amendment to the United States Constitution.[36] Compared to EU "regulated self-regulation",[37] the primary method by which free-speech encroachments are made is by modifying digital platforms' content moderation policies, or Terms of Use. Importantly, while our digital media environment has freed speakers from dependence on older gatekeepers epitomized by editorial processes of print journalism, the shift from a "broadcasting" to a "participatory" communication model has introduced a new, highly interactive communication entity – the digital platform.[38] Whether in the EU or North America, our increasing reliance on these new gatekeepers has proven to be highly problematic.[39] Offering states and private actors not only new opportunities for control and surveillance,[40] these digital platforms engender unprecedented and unforeseen tensions between their business models and duties to respect fundamental and human rights, a phenomenon that has recently crystallized in America.[41]

Constitutional challenges and critiques

Many of these issues are now being litigated before the US Supreme Court in *Moody v NetChoice, LLC*.[42] Recently, over 100 bills have been proposed in state legislatures purporting to regulate social media platforms' content moderation policies.[43] On 21 September 2022, the Attorney General for the State of Florida petitioned the US Supreme Court for a writ of certiorari to review a judgment of the Eleventh Circuit Court of Appeals, which declared significant portions of Florida's new common carrier free speech statute unconstitutional.[44] In Senate Bill 7072,[45] Florida sought to regulate the "unlawful acts and practices" of social media platforms in censoring political and dissenting content by requiring them to divulge the how and why of their censorship decisions, and to host speech that they otherwise would not. Specifically, as to disclosure, the Florida Act requires platforms to "[…] publish the standards, including detailed definitions, it uses or has used for determining how to censor, deplatform, and shadow ban".[46] As to mandatory hosting rules, the Act leaves social media platforms free to adopt otherwise lawful content- and viewpoint-discriminatory standards, but requires them to apply whatever "[…] censorship, deplatforming, and shadow banning standards in a *consistent* manner among its users […]".[47] Evidencing the great importance of this case, many other states remain "waiting in the wings", as evidenced by the multi-jurisdictional Amicus brief filed in support of Petitioner, State of Florida.[48]

Although both parties joined issue on granting leave to appeal, the main disputed questions raised for consideration in *Moody* include:

- Whether hosting on a digital platform constitutes "speech" or "editorial discretion";
- Whether a censorship right can be extracted from the First Amendment;
- Whether digital platforms can or should be regulated as "common carriers";[49]
- Whether Congress authorized platforms to engage in content- and viewpoint-based discrimination under section 230 CDA;
- Whether the Dormant Commerce Clause and section 230 CDA are preemptive.

Perhaps most interestingly, Columbia Law Professor *Philip Hamburger* filed an Amicus brief urging the US Supreme Court to proceed cautiously in the light of two deficiencies in the appeal record. First, *Hamburger* keenly observed that by applying for a preliminary injunction against enforcement of the Florida Act before suffering actual harm, the platforms framed their lawsuit "[…] in a posture that leaves the speech rights of ordinary Americans *unrepresented*".[50] Second, and related, the case arose on an appeal record devoid of discovery evidence "[…] on the depth of government involvement in the censorship" attributed to digital platforms alone.[51] According to *Hamburger,* this missing evidence is "crucial" because "[i]t confirms […] that the case is centrally about the free speech of individuals, whose rights are not represented",[52] and it demonstrates "[…] the compelling need for common carrier laws, such as the Florida and Texas free speech statutes, to prevent government from privatizing its censorship".[53] The absence of a full evidentiary record of privatized government censorship is made all the more worrisome given *Hamburger*'s conviction that "[t]he jurisprudence of this Court has yet to catch up with the realities of how government uses private organizations to violate constitutional rights with impunity".[54]

In the end, if the US Supreme Court takes up these challenges in *Moody*, the law of Internet regulation is likely to be changed materially, not only for the United States, but worldwide.

2. Canada's "hybrid" regulatory model

Compared to the EU and the United States of America, Canada has embraced a more consultative, "multi-stakeholder" approach to online harms. Currently awaiting statutory implementation of advice provided by experts composed of specialists in platform governance, content regulation, civil liberties, tech regulation, and national security, Canada's government has avoided a fixed timeframe for its new regulatory framework, vowing instead to take whatever time necessary to meet the challenge of "[…] getting the legislation right".[55]

Bill C-36, "technical discussion paper", and expert consultations

Canada's most recent hate speech legislation was introduced in 2021. Called Bill C-36,[56] it aimed to amend the Canadian Human Rights Act to make it a discriminating practice "[…] to communicate or cause to be communicated hate speech by means of the Internet or other means of telecommunications […]".[57] Besides exempting private online communications,[58] the proposed amendments – like the American "market self-regulation" model – included extensive safe harbors for digital platforms.[59] Subsection 13(4), for example, excluded certain "telecommunications service providers' from its definition of 'communication of hate speech",[60] and subsection 13(7) exempted the Bill's application to "online communication service providers" altogether.[61] Combined with an equivocal definition of "hate speech",[62] the Bill left potential victims of online harms with

a limited and ineffective range of quasi-judicial remedies, including cease and desist orders and more conventional awards of compensatory and punitive damages.[63] Despite its aim of providing an "important part" of Canada's online regulatory framework, Bill C-36 was interrupted by the 2021 federal election, and has since stalled at first reading in Canada's House of Commons.[64]

Along with Bill C-36, the Canadian government presented a "technical discussion paper" as part of its proposed regulatory framework,[65] which provides greater clues as to the country's regulatory goals. Borrowing a page from Germany's *NetzDG*, it endorsed a mandatory 24-hour takedown requirement for harmful content, backstopped by a federal "last resort" power to block non-compliant digital platforms. Additional aspects included:[66]

- Compelling platforms to provide data on algorithmic filtering and blocking, including rationales for acting on flagged posts;
- Obliging websites to employ better means for identifying and alerting authorities of illegal content, including preserving user data for future legal action;
- Creating a new system for appealing platforms' content moderation decisions;
- Employing severe sanctions for non-compliance, including fining companies up to five percent of their global revenue, or $25 million, whichever is higher.

Finally, a new "Digital Safety Commission of Canada" was proposed, which would preside over this regulatory environment with powers – similar to EU's DSA – to issue binding "takedown" orders to online platforms.

Responding to concerns that this proposal did not properly respect freedom of expression,[67] politicians announced plans to go back to the proverbial drawing board. Mindful of the ever-increasing complexities of online regulation, government officials proceeded on the basis that future regulations would not be a "panacea" for rectifying offensive content, but would be only "one piece of a bigger puzzle".[68]

After convening an expert panel in 2022, some of its chief proposals for Canada's revised framework were that the legislation should:[69]

- emphasize risk management and human rights protections, and be flexible and adaptable to avoid becoming quickly obsolete;
- incorporate strong commitments to digital literacy and public education;
- establish clear consequences for non-compliance;
- consider systemic biases and harm associated with bots, algorithms, and AI;
- incorporate a suitable process for appealing content moderation decisions.

At last, as reflected by the growing regulatory heterogeneity described above, Canada's expert panel disagreed on several vital issues, such as the definition of "harmful content", mandatory content removal, the suitability of a 24-hour takedown requirement, the need for and feasibility of an independent review body, proactive or general platform monitoring, mandatory reporting to law enforcement authorities, platform immunity for speech torts, tailoring regulatory obligations to platform size or risk, and the way to deal with fake news and disinformation.[70]

IV. Mounting Regulatory Tensions

From a comparative perspective, European and North American responses to harmful online content provide valuable insights into the nature and scope of regulatory challenges worldwide. First, the unique structural features of our digital media environment raise significant and unanticipated epistemological concerns for online regulators, requiring a new paradigm for bringing together a multitude of variables into an enhanced understanding of our online world. Second, differences in human rights protection and constitutional structure present difficult challenges for online regulators, requiring keen sensitivity to political and constitutional contexts for optimizing regulatory calibration. Third, the unprecedented power of digital platforms incentivizes privatized government censorship which, along with existing economic incentives driving platform censorship, increasingly imperils the quality and quantity of public discourse.

1. Digital media ecology and medico-legal integration

a) Restructured media ecology

The advent of the Internet and social media has triggered a seismic shift in our contemporary media ecology,[71] transferring human discourse production onto a new medium and drastically altering its structure and dynamics. This transfer of ever greater portions of our lives online has given rise to many unanticipated epistemological concerns.[72] From the emergence of augmented and virtual reality, and the looming prospect of an all-encompassing Metaverse,[73] to the dangers of "link rot" (i.e. hyperlinks ceasing to work) and the weakening of humanity's knowledge base,[74] we are seeing a rapid intensionalization of our infosphere.[75] In less than a generation, humanity has effectively rewritten nature's code.

This "digital town square" raises many regulatory challenges. The US Supreme Court has sensibly accepted that when deciding free speech cases, it does "[…] not mechanically apply [a] rule used in the pre-digital era" to technology of today.[76] In *Biden v Knight First Amendment Institution at Columbia University*,[77] a recent case involving President Donald Trump's Twitter conduct, Justice *Clarence Thomas* wrote a thoughtful concurring opinion that may well influence future thinking on regulating digital platforms. Besides endorsing anti-discriminatory common carrier laws, he stressed that the principal difficulty of platform regulation is that "[…] applying old doctrines to new digital platforms is rarely straightforward".[78] As evidenced by the pending litigation in *Moody,* Justice *Thomas* rightly predicted that the Court "[…] will soon have no choice but to address how our legal doctrines apply to highly concentrated, privately owned information infrastructure such as digital platforms".[79]

Importantly, the full extent of risks posed by our modern free speech infrastructure is gradually being revealed. Besides acknowledging that our jurisprudence has yet to catch up with our digital media ecology more broadly, courts and legislatures are only now beginning to heed the admonitions of legal scholars who have long warned of increasing privatization of government censorship. Over a decade ago, Professor *Jack Balkin* cautioned that so-called "new-school" regulatory techniques associated with modern digital media – which include controlling digital networks and auxiliary services like search engines, payment systems, and advertisers – present heightened risks of government co-optation and censorship of private owners of our global media infrastructure.[80] Accompanied by rising awareness that "[p]latform control means content control",[81] *Balkin* cautioned that our contemporary media environment effectively functions as an "[…] ingenious system of private prior restraint [that] achieves all of the cost- and burden-shifting effects of traditional prior restraint without the need for an official government licensing system or a judicial injunction".[82] Given mounting evidence that public discourse is now subject to "[…] the most extensive system of censorship in […] history",[83] there is an urgent need for new ideas and paradigms to assist in formulating effective "[…] *structural* obstacles to the privatization of censorship".[84]

b) Insights from theoretical biology and medicine

Reconciling dislocations between old legal doctrine and new media requires restructuring and reordering the relations between affected stakeholders in our new digital environment. As anticipated by legal realists, medical science may provide valuable insights for formulating a more integrative model of Internet regulation.

Consistent with earlier trends towards intellectual synthesis embraced by Justices *Holmes* and *Cardozo*, in 1993 molecular biologist Professor *Richard Strohman* thoughtfully explored the possibility of a growing crisis in medical science and theoretical biology.[85] While admitting that cellular mechanisms were amply understood, *Strohman* argued that medicine's dominant model of genetic determinism – that complex human diseases and behaviors are reducible to purely genetic influences – was increasingly unable to contend with newer findings of biological complexity, necessitating a new and more comprehensive theory of living systems. This urgency for developing a new medical paradigm was noted earlier by Dr *George Engel*.[86] In *Engel*'s view, medicine was in crisis because of its adherence to a disease model that was no longer adequate for the profession's scientific tasks and social responsibilities. Notably, while medical education had grown increasingly proficient in conveying to physicians sophisticated scientific knowledge about the body and its abnormalities, it had failed to give corresponding attention to the psychological and social aspects of illness and treatment.

At their respective levels of abstraction, *Engel* and *Strohman* questioned emerging trends towards biological reductionism and elementalism that have since come of age in our modern era. In their place, they argued for a new "biopsychosocial" paradigm, a transactional, holistic, analogical, and probabilistic approach to health and disease reflecting mounting evidence that "[…] the pathogenesis of disease involves a series of negative and positive feedbacks with multiple simultaneous and sequential changes potentially affecting any system of the body".[87] Among its implications, this model required physician-lawyers to explore complex relationships between social stress and bodily experience, to study how the corporealization of cultural experience occurs, and to determine our adaptive limits to environmentally-determined stressors.

Perhaps most importantly, this new medical model implicated physicians in wider political debates from which the current conceptualization of disease might have insulated them, a point illustrated analogously by containing the tensions and challenges of global Internet governance within the rubric of more conventional methods and approaches to digital media regulation.

2. Fundamental rights protection and constitutional structure

As in *Engel*'s biopsychosocial paradigm, a renewed commitment to intellectual synthesis in our Internet govern-

ance era requires that we include a broader array of factors impacting digital media regulation. As seen above, two additional comparative law factors are differences in fundamental rights protection, and variances in constitutional structure.

One of the most troubling aspects of global Internet regulation is the considerable variation in free speech protection. Although DSA purports to be a "complete code" for all 27 EU Member States, not only does hate speech remain undefined, but there exists an increasing overlap with established public libel principles protecting speech that "[…] *offend[s]*, *shock[s]*, or *disturb[s]* the State or any sector of the population".[88] Perhaps most worryingly, the US Constitution protects an enlarged scope of "offensive" speech under the First Amendment, including hate speech.[89] Much of what DSA intends to regulate as "illegal content" is constitutionally protected in America, a problem exacerbated by the "all-or-nothing" nature of platform posting. Moreover, regardless of jurisdiction, digital intermediaries continue to exclude categories of problematic speech by modifying their subscribers' Terms of Use in potentially violable ways. Globally, we are confronting profound regulatory dilemmas about striking an appropriate balance between individuals' interests in free speech, and maintaining a robust and functional public sphere.

The second unsettling aspect of global Internet regulation is discrepancies in constitutional structure. Even if we could reconcile differences in global free speech protection, successful regulatory calibration requires responding to varying political and constitutional designs, a process heavily dependent upon comparative methods. Recent comparative law scholarship establishes that changes in presidential and parliamentary governments, federal and unitary structures, mechanisms of legislative scrutiny, electoral systems, and the nature and extent of judicial review all have well-documented influences on regulatory dynamics in modern democracies.[90] The emergent field of public accountability scholarship has further shown that established democracies have institutionalized a broad array of accountability mechanisms, which interrelate and have important aggregate effects, especially on holding power to account.[91] These insights are particularly relevant given the underreported effects of our digital media ecology on the promotion and privatization of government censorship.

In the end, given the vast number of moving parts in online regulation, any "one-size-fits-all" approach or premature attempts at "harmonization" would appear to be structurally unsound.

3. Economic and political bases of digital censorship

Perhaps the most important aspect of global online regulation is the economic motives of digital platforms themselves. Consider the operation of today's digital marketplace. As a rule, our networked economy's basic structure incentivizes digital intermediaries to make their platforms a welcome place and experience. Naturally, "[t]he goal is to attract and retain as many [online] users as possible".[92] Economic success, then, is a function of acceptance and community norms – what sells will be what the community deems desirable. As explained by *Peters* and *Johnson*, "[…] if community norms dictate that certain speech does not sell (i.e., its presence deters individuals from using a platform), that speech is not likely to survive […]".[93] If left to the market, platforms will not long tolerate speech that damages their commercial interests. Importantly, speech that might brook disagreement or start an argument – speech that might "offend", "shock", or "disturb", for instance – is unlikely to be "liked", "shared", or otherwise promoted by users and intermediaries. As measured by the click-through advertising rates of online users,[94] the main regulatory challenge conventionally linked with this business model is that it often conflicts with human rights norms, particularly freedom of expression. This proclivity of digital platforms to censor otherwise protected speech in their Terms of Use – even under the First Amendment of the US constitution – speaks to the power of the economic motives driving the increasing phenomena of overfiltering and overblocking.

Besides encouraging filtering and blocking of "problematic" content, these technological and economic forces ultimately manifest in deeper *structural* threats to democracy. As cautioned by Professor *Balkin* in 2012, digital platforms that rely on advertising and online payment systems are increasingly induced to install filters and to continually police and remove "problematic" content. Besides exposing online users to an endless algorithmic selection of "bias-affirming materials that by turns soothe and provoke" further online engagement,[95] we are only now confronting the possibility that the effective aim and result of our digital free speech infrastructure was "[…] to induce companies to engage in *collateral censorship* […]".[96] As stressed by *Hamburger* in the *Moody* litigation presently before the US Supreme Court (see above III.1.), whether censoring "[…] academic papers, reports of medical cases, passionate disagreements, moderate colloquies, videos, and cartoons",[97] because governments around the world have taken strong positions, particularly on issues of science and medicine, "[…] the censorship of dissenting views on these matters *is* the suppression of political opposition".[98] As a result, serious threats to public discourse remain largely concealed, and thus more difficult to diagnose and regulate.

V. Conclusion

In many ways, regulatory responses to ever-rising threats of offensive online content reflect well-intentioned, but hasty attempts to saddle the law with the burden of tasks that have had increasingly little to do with its existing methods, instruments, and theories. As argued in this article, limitations associated with our online regulatory frameworks can be better understood – perhaps mitigated, or even avoided altogether – by integrating pertinent insights from the natural and medical sciences. Foremost among these insights has been adopting a new scientific paradigm to bring together a multitude of variables into an enhanced understanding of our online world. Inspired by *Engel's* biopsychosocial model, attempts to explain a complex phenomenon, such as harmful online content and its legal regulation, necessitate comprehensive investigations of socio-political levels of abstraction for clues as to its dysfunctions. In retrospect, earlier application of these insights might have invited difficult questions about the nature of digital intermediaries and their economic interests, including their relationship to the unique technological structure of our digital public sphere.

Such a systems-inspired approach may have even avoided the largely unexplored regulatory dichotomy that persists to this day. Whether employing a "notice-and-takedown" or "market self-regulation" model, we have yet to face squarely the possibility that the more we focus on regulating "offensive speech", the deeper we entrench the technical infrastructure supporting privatization of government censorship. Among the many takeaways from Professor *Hamburger*'s admonitions is that by neglecting systematic censorship worldwide, we may be fighting only symptoms of online disease, not its structural causes. Incorporating mounting evidence of the economic incentives driving digital platforms thus has vital diagnostic and prescriptive value. While lending credibility to allegations of privatized government censorship, it also strengthens the case for adopting common carrier legal principles, or other structurally effective barriers to privatized censorship. By restricting our frame of reference to speech rights and offensive content – regardless of regulatory model – we may be "looking through the wrong end of the telescope", and missing an important opportunity to perhaps cure what really ails us – before it is too late.

In the end, as evidenced by the growing epistemic, technical, economic, and politico-legal challenges of digital media regulation, our best prospect for their reconciliation will be exercising our increasingly untapped capacity for intellectual synthesis that our forebears seem to have understood more acutely in the past. For whatever else it may do, it must inevitably result in healthy criticism, wider views, new fields of research, and greater activity on the part of those interested in questioning why, in our modern age of unprecedented wealth and technological advancement, more civil and open public discourse does not prevail.

Dr. Randall Stephenson, LL.M. (Columbia), M.St., D.Phil. (Oxon)
Senior Researcher, Public Law Department, Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

Dr. Johanna Rinceanu LL.M. (Washington, D.C.)
Senior Researcher, Criminal Law Department, Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

1 R. A. Posner, *The Essential Holmes: Selections from the Letters, Speeches, Judicial Opinions, and Other Writings of Oliver Wendell Holmes Jr*, 1992, p. 184.
2 B. Cardozo, "Anniversary Discourse: What Medicine Can Do for Law", (1929) 5 *Bulletin of the New York Academy of Medicine*, 581.
3 R. Pound, "The Lawyer as a Social Engineer", (1954) 3 *Journal of Public Law*, 292. Like Cardozo, Pound encouraged lawyers to heed insights from other disciplines to become effective "social engineers" committed to real-world problem solving. See also J. Pope, "The Unfolding Unity" (1954) *3 Journal of Public Law*, 319.
4 B. Cardozo, *op. cit.* (n. 2), p. 583.
5 B. Cardozo, *op. cit.* (n. 2), p. 583.
6 B. Cardozo, *op. cit.* (n. 2), p. 584. On medico-legal integration, see also J. M. Gibson and R. L. Schwartz, "Physicians and Lawyers: Science, Art, and Conflict", (1980) 6 *American Journal of Law & Medicine*, 173; H. W. Smith, "Integration of Law and Medicine", (1963) 14 *Syracuse Law Review*, 550; H. W. Smith, "Scientific Proof and Relations of Law and Medicine", (1943) 10 *University of Chicago Law Review*, 243. Predating Justice Cardozo's proposal, the German physician Rudolf Virchow famously referred to physicians as "natural attorneys of the poor", once stating that "medicine is a social science, and politics is nothing else but medicine on a large scale". See R. Virchow, "Der Armenarzt", (1848) 18 *Die Medicinische Reform* 125, 125.
7 H. W. Smith, *op. cit.* (n. 6), p. 555.
8 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ LI277/1.
9 For Canadian regulations, see Bill C-36, An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda,

hate crimes and hate speech), 2nd Sess, 43rd Parl, 2020–2021, ss 12–13 (first reading 23 June 2021). See also Department of Canadian Heritage, "*The Government's Commitment to Address Online Safety"*, Government of Canada, <https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html> accessed 10 March 2023.

10 I. Illich, *Medical Nemesis: The Expropriation of Health*, 1975, p. 165. In *Medical Nemesis*, "iatrogenesis" was coined to describe the causation of disease or harmful complications attributable to human or medical activity, including diagnosis, intervention, error, or negligence. Illich referred to three distinct but interrelated forms of iatrogenesis operative at progressively higher levels of abstraction – clinical, social, and structural.

11 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) from 1 September 2017 (BGBl I p 3352).

12 Digital Services Act *op. cit.* (n 8).

13 For criticisms of NetzDG, see J. Mchangama, „The War on Free Speech: Censorship's Global Rise", (2022) 101 *Foreign Affairs* 117, 123–24; J. Rinceanu, „Menschenrechte in der digitalen Krise" in M. Engelhart and H. Kudlich and B. Vogel (eds.), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag*, 2021, p. 831. See also H. Tworek and P. Leerssen, "An Analysis of Germany's NetzDG Law", (2019) *First session of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*.

14 Under §§ 3(2)(2)–(3) NetzDG, "manifestly unlawful" content must be deleted or blocked within 24 hours, whereas all other "unlawful content" within seven days upon receipt of a complaint.

15 § 1(3) NetzDG.

16 § 3(2)(5) NetzDG.

17 § 2(1) NetzDG.

18 § 3a NetzDG.

19 Many nations, like Ethiopia, Pakistan, Turkey, Russia, Belarus, Mali, Morocco, Nigeria, Cambodia, Indonesia, and Kyrgyzstan, that followed NetzDG's example, are flawed democracies or authoritarian states that do not have Germany's rule of law safeguards and free speech protections. See J. Mchangama and N. Alkiviadou, "*The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship – Act Two*", 2020, p. 21.

20 According to Art. 93(2), DSA shall apply from 17 February 2024.

21 Art. 1 DSA.

22 DSA distinguishes three categories of digital intermediary services, namely, conduit, caching, and hosting. See Art. 3(g) DSA.

23 Art. 74 DSA and Recital 117. Fines not exceeding 6% of total corporate revenue can be imposed on "very large" platforms and search engines under DSA.

24 Provisions on the "notice-and-action" mechanism are anchored in Art. 16 et seq. DSA.

25 Art. 22 DSA.

26 Art. 17 DSA.

27 Art. 17(3)(f) DSA.

28 Art. 18 DSA.

29 Art. 8 DSA.

30 Recital 9 DSA.

31 See generally G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability*, 2020.

32 Communications Decency Act, 47 USC § 230 (1996). See generally E. Goldman, "An Overview of The United States", in G. Frosio, *op. cit.* (n. 6), p. 155.

33 CDA, *op. cit*. (n. 32), § 230(c)(1) (emphasis added).

34 E. Goldman, "Why Section 230 is Better than the First Amendment", (2019) 95 *Notre Dame Law Review* Reflection, 33, 37.

35 See M. Ammori, "The 'New' *New York Times*: Free Speech Lawyering in the Age of Google and Twitter" (2014) 127 *Harvard Law Review,* 2259, 2287.

36 US Const Amend I. The First Amendment reads: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". See also J. Kamatali, "Limits of the First Amendment: Protecting American Citizens' Free Speech in the Era of the Internet and the Global Marketplace of Ideas", (2015) 33 *Wisconsin International Law Journal,* 587. The US Supreme Court has exempted numerous categories of speech from First Amendment protection, including: Obscenity, fighting words, defamation, child pornography, fraud, and incitement to imminent lawless action. See V. L. Killion, Congressional Research Service, IF11072, *The First Amendment: Categories of Speech* (2019).

37 See e.g. H. J. Kleinsteuber, "The Internet between Regulation and Governance", in: C. Möller and A. Amouroux (eds.), *The Media Freedom Internet Cookbook*, 2004, p. 61, 63.

38 See generally R. K. Logan, *Understanding New Media: Extending Marshall McLuhan*, 2d ed., 2016, pp. 27–74.

39 See e.g., J. Peters and B. Johnson, "Conceptualizing Private Governance in a Networked Society", (2016) 18 *North Carolina Journal of Law and Technology*, 15.

40 See e.g. J. M. Balkin, "Old-School/New-School Speech Regulation", (2014) 127 *Harvard Law Review*, 2296; J. M. Balkin, "The First Amendment is an Information Policy", (2012) 41 *Hofstra Law Review*, 1. See also L. DeNardis, *The Global War for Internet Governance*, 2014, p. 17, who also emphasises the fundamental importance of the Internet's free speech infrastructure.

41 See eg R. L. Weaver, *From Gutenberg to the Internet: Free Speech, Advancing Technology, and the Implications for Democracy,* 2nd ed., 2019.

42 See US Supreme Court, 21 September 2022, *Moody v NetChoice, LLC,* No. 22-277; *NetChoice, LLC v Moody* 34 F4th 1196 (11th Cir 2022), *aff'g* No 4:21-cv-00220 (ND Fla 2021).

43 D. Harwell, "Jan. 6 Twitter witness: Failure to curb Trump spurred 'terrifying' choice" *The Washington Post* <https://www.washingtonpost.com/technology/2022/09/22/jan6-committee-twitter-witness-navaroli/> accessed 11 March 2023.

44 Brief for Petitioner, US Supreme Court, 21 September 2022, *Moody v NetChoice, LLC,* No. 22-277.

45 Florida Statutes § 501.2041 (Florida Act).

46 *Op. cit*. (n. 45), § 501.2041(2)(a).

47 *Op. cit*. (n. 45), § 501.2041(2)(b) (emphasis added).

48 Brief of *Amici Curiae* States of Ohio, Alabama, Alaska, Arizona, Arkansas, Idaho, Iowa, Kentucky, Mississippi, Missouri, Montana, Nebraska, South Carolina, Tennessee, Texas, and Utah in Support of Petitioners, US Supreme Court, 21 September 2022, *Moody v NetChoice, LLC,* No. 22-277. Petitioners reported that, at last count, "lawmakers in 34 states" are considering laws regulating social media platforms to prevent unfair censorship. See, Brief for Petitioner, *op. cit.* (n. 44), p. 13.

49 For thorough analyses of common carrier laws and their ability to counter social media platforms leveraging economic might into enhanced political power and censorship, see G. M. Dickinson, "Big Tech's Tightening Grip on Internet Speech", (2022) 55 *Indiana Law Review*, 101; E. Volokh, "Treating Social Media Platforms like Common Carriers?", (2021) 1 *Journal of Free Speech Law,* 377; G. Lakier, "The Non-First Amendment Law of Freedom of Speech", (2021) 134 *Harvard Law Review*, 2299.

50 Brief of Professor P. Hamburger as Amicus Curiae in Support of Neither Party, US Supreme Court, 21 September 2022, *Moody v NetChoice, LLC,* No. 22-277, p. 3 (emphasis added).

51 Brief of Professor P. Hamburger, *op. cit.* (n. 50).
52 Brief of Professor P. Hamburger, *op. cit.* (n. 50), p. 9.
53 Brief of Professor P. Hamburger, *op. cit.* (n. 50).
54 Brief of Professor P. Hamburger, *op. cit.* (n. 50), p. 16–17. See also K. Langvardt, "Regulating Online Content Moderation", (2018) 106 *Georgetown Law Journal*, 1353, 1355.
55 See generally R. Aiello, "Where does the Liberal promise to address harmful online content stand?", CTVNews.ca, <https://www.ctvnews.ca/politics/where-does-the-liberal-promise-to-address-harmful-online-content-stand-1.6048720> accessed 11 March 2023.
56 See Bill C-36, *op. cit.* (n. 9), ss 12–23.
57 Bill C-36, *op. cit.* (n. 9), ss 13(1).
58 Bill C-36, *op. cit.* (n. 9), ss 13(5).
59 Bill C-36, *op. cit.* (n. 9), ss 13(4), 13(7).
60 Bill C-36, *op. cit.* (n. 9), ss 13(4). This subsection exempted "telecommunications services providers" as defined in subsection 2(1) of Canada's Telecommunications Act.
61 Bill C-36, *op. cit.* (n. 9), ss 13(7).
62 Bill C-36, *op. cit.* (n. 9), ss 13(9), 13(10).
63 Bill C-36, *op. cit.* (n. 9), s 19.
64 Bill C-36, *op. cit.* (n. 9).
65 Department of Canadian Heritage, "*The Government's Commitment to Address Online Safety: Technical Paper*", Government of Canada, <https://www.canada.ca/en/canadian-heritage/ campaigns/harmful-online-content/technical-paper.html> accessed 11 March 2023.
66 Department of Canadian Heritage, *op. cit.* (n. 65).
67 M. Geist, "Tracking the Submissions: What the Government Heard in its Online Harms Consultation (Since It Refuses to Post Them)", *MichaelGeist.ca*, <https://www.michaelgeist.ca/2021/10/tracking-the-submissions-what-the-government-heard-in-its-online-harms-consultation-since-it-refuses-to-post-them/> accessed 11 March 2023.
68 R. Aiello, *op. cit.* (n. 55).
69 Department of Canadian Heritage, *"Expert Advisory Group: Concluding Workshop Summary",* Government of Canada, <https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/concluding-summary.html> accessed 11 March 2023.
70 Department of Canadian Heritage, *op. cit.* (n. 69).
71 See L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, 2014. The ubiquity and vital role of social media has prompted the US Supreme Court to declare it "the modern public square". See US Supreme Court, *Packingham v North Carolina* 137 S Ct 1730, 1732 (2017).
72 See L. Floridi, "Soft Ethics and the Governance of the Digital", (2018) 31 *Philosophy and Technology*, 1. *Floridi* contends that we no longer live online or offline – but *onlife*.
73 See M. Ball, "Framework for the Metaverse: The Metaverse Primer", *MatthewBall.vc*, 29 June 2021, <https://www.matthewball.vc/all/forwardtothemetaverseprimer> accessed 11 March 2023.
74 J. Zittrain, "The Internet is Rotting: Too much has been lost already. The glue that holds humanity's knowledge together is coming undone", *The Atlantic*, <https://www.theatlantic.com/technology/archive/2021/06/the-internet-is-a-collective-hallucination/619320/> accessed 11 March 2023.
75 Even in the 1960s and 1970s, Marshall McLuhan foresaw the next era in communications technology leading to an epistemic "hyperreality" not unlike the Metaverse. See R. K. Logan, *op. cit.* (n. 38), p. 46.
76 US Supreme Court, *Riley v California* 573 US 373 (2014), 406–07 (Alito J, concurring).
77 US Supreme Court, *Biden v. Knight First Amendment Institute,* 141 S Ct 1220 (2021) (Thomas J, concurring).
78 US Supreme Court, *op. cit.* (n. 77), 1221.
79 US Supreme Court, *op. cit.* (n. 77).
80 See J. M. Balkin, *op. cit.* (n. 40).
81 A. Tutt, "The New Speech", (2014) 41 *Hastings Constitutional Law Quarterly*, 235, 249.
82 J. M. Balkin, *op. cit.* (n. 40), p. 2326.
83 Brief of Professor P. Hamburger, *op. cit.* (n. 50), p. 25.
84 Brief of Professor P. Hamburger, *op. cit.* (n. 50), p. 16 (emphasis added).
85 R. C. Strohman, "Ancient Genomes, Wise Bodies, Unhealthy People: Limits of a Genetic Paradigm in Biology and Medicine", (1993) 37 *Perspectives in Biology and Medicine*, 112, 112.
86 G. L. Engel, "A Unified Concept of Health and Disease", (1960) 3 *Perspectives in Biology and Medicine*, 459; G. L. Engel, "The Need for a New Medical Model: A Challenge for Biomedicine", (1977) 196 *Science*, 129.
87 G. L. Engel, "A Unified Concept of Health and Disease", *op. cit.* (n. 86), p. 485.
88 ECtHR, 7 December 1976, *Handyside v United Kingdom*, 1 EHRR 737 [49] (emphasis added). See also ECtHR, 8 July 1986, *Lingens v Austria*, 8 EHRR 407; ECtHR, 23 April 1992, *Castells v Spain*, App. no. 11798/85. For recent commentary on this point, see J. Mchangama and N. Alkiviadou, "Hate Speech and the European Court of Human Rights: Whatever Happened to the Right to Offend, Shock or Disturb?", (2021) 21 *Human Rights Law Review*, 1008.
89 See generally J. Kamatali, *op. cit.* (n. 36).
90 See e.g., R. Stephenson, *A Crisis of Democratic Accountability: Public Libel Law and the Checking Function of the Press*, 2018.
91 See e.g., M. Bovens and others (eds.), *The Oxford Handbook of Public Accountability*, 2014; K. Strøm and others (eds.), *Delegation and Accountability in Parliamentary Democracies*, 2008; R. Mulgan, *Holding Power to Account: Accountability in Modern Democracies*, 2003; A. Schedler and others (eds.), *The Self-Restraining State: Power and Accountability in New Democracies*, 1999.
92 J. Peters and B. Johnson, *op. cit.* (n. 39), p. 65.
93 J. Peters and B. Johnson, *op. cit.* (n. 39), p. 65.
94 M. Lavi, "Content Providers' Secondary Liability: A Social Network Perspective", (2016) 26 *Fordham Intellectual Property Media & Entertainment Law Journal*, 855, 935–36 fn. 316.
95 K. Langvardt, "A New Deal for the Online Public Sphere", (2018) 26 *George Mason Law Review*, 341, 358.
96 See J. M. Balkin, *op. cit.* (n. 40), p. 2324 (emphasis added).
97 Brief of Professor P. Hamburger, *op. cit.* (n. 50), p. 6.

Why a Human Court?

On the Right to a Human Judge in the Context of the Fair Trial Principle

I care very little if I am judged by you or by any human court; indeed, I do not even judge myself.

(1 Corinthians 4:3)

Marcin Górski

For centuries, "doing justice" has been a fundamentally anthropocentric effort: Humankind has been placed at the centre of emerging paradigms and systems such as (quite self-evidently) human rights, constitutionalism, and – gradually – also international law. In addition to focusing adjudication on individuals and their litigated interests, this has meant an administration of justice taking the form of human activity. The advent of automated public decision-making, including adjudication based on artificial intelligence (AI) tools, has raised concerns of possible shortcomings and abuses of justice resulting from their application. So is it time to change this anthropocentric mindset? More specifically, has the time come to replace human judges with AI? Can we do without them? Technological progress, rather than legal considerations, is likely to decide the fate of the anthropocentric outlook. This is why this essay aims to focus on the future of human judges. The proposition put forward is that courts cannot operate without a human element, less so because of technical constraints, but rather in light of the modern understanding of the right to a fair trial.

I. Contemporary Understanding of the Right to a Fair Trial and the Potential Impact of Artificial Intelligence

The notion of the right to a fair trial has evolved over time. Taking Poland as an example, the beginnings of the right to a fair trial were rooted in the privileges of the gentry (or, oversimplified, the aristocracy). This dates back to the XV century and was first expressed in the statutory limitations of the royal power of expropriation and the rule of subjecting the gentry only to adjudication based on a written law (the so-called *Czerwińsk Privilege* of 1422), which was accompanied by the *neminem captivabimus nisi iure victum* principle. The right to a fair trial was strengthened by the first Constitution of 1791 and further developed during the Second Republic (1918–1939). Gradually abolished during the communist era (roughly 1944–1989), the right to a fair trial was revived as early as the late 1980s and "flourished" again with the rise of democracy after the collapse of the communist rule in 1989. Sadly, it took a great hit after 2015 under the present far-right government.[1]

More generally, the more power is (at least allegedly) vested with the judiciary (both international and national), the more weight the right to a fair trial carries.[2] This ratio is like a litmus test of democracy where "fair-trial guarantees […] are guided by the aim of upholding the fundamental principles of the rule of law and the separation of powers."[3]

Fundamental international documents devoted to human rights share a relatively common definition of the right to a fair trial: the Universal Declaration of Human Rights (UDHR) in Articles 8 and 10, the International Covenant on Civil and Political Rights (ICCPR) in Art. 14, the American Convention on Human Rights in Art. 8, (to a lesser extent) the African Charter of Human and Peoples' Rights in Art. 7, the European Convention on Human Rights (ECHR) in Arts. 6 and 13, and the Charter of Fundamental Rights of the European Union (ChFR) in Art. 47 – all rather uniformly refer to nine elements of the right to a fair trial, i.e. fairness, public hearing, reasonable time, independence and impartiality of the trial court, lawfulness of judicial appointment, right of a party to be represented and to have legal aid free-of-charge, and (implicitly – e.g. in the ECHR, or explicitly – e.g. in the ChFR) the right to effectiveness of judicial protection. The national constitutions of the European states all refer to the safeguards of the right to a fair trial in much the same way.[4]

Perhaps one may even claim that the notion of a fair trial, as matters stand, amounts to a pre-existent[5] (or extant) constitutional notion, i.e. a concept that does not require defining because everyone is already familiar with it. As for these nine criteria at the heart of a fair trial, it seems pretty clear that an AI-driven judiciary is likely to have a positive effect on the expeditiousness of proceedings whilst making no difference to the right to legal representation or legal aid, or to the right to a public hearing (i.e. access of the public to the hearing and to the pronouncement of judgments[6]). However, what remains unclear is whether the introduction of an AI-based judiciary might adversely

affect the ("sub") rights to independence and impartiality (and lawful establishment) of the trial court or to fairness of proceedings. This will be discussed further in the next sections.

1. Independence, impartiality, and lawfulness of establishment of the trial court

Legal scholars have raised certain objections against the use of AI in the courtroom concerning judicial independence[7]. For example, *Nowotko* held that "the court which issues judgments by means of an IT system based on artificial intelligence cannot be independent in the meaning of independence in adjudication"[8], and *Gentile* suggested that

> "any influence exercised by a state's executive or the legislative, for instance, over data centres used to digitise judicial decisions, the selection of the training data for neural systems, or the very design of the algorithm used in the courtroom would be liable to raise doubts about the court's independence".[9]

These concerns are apparently shared by the European Commission, which proposed a draft Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) in 2021.[10] The proposal classifies "AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts" as "high-risk AI systems" and (in Article 14) aims at subjecting them to human supervision "during the period in which the AI system is in use" in order to protect fundamental rights. This approach is based on the noticeable belief in the quality of the human judiciary and – more broadly – on the anthropocentric orientation of contemporary constitutionalism[11] and, gradually, international law as well[12].

The idea behind these concerns seems to be that if an algorithm delivers a judgment (or participates therein in the decision making by providing decisive data), it is not "independent" from the humans who developed the algorithm, nor from the data contained and managed by an automated system. The judgment, instead of being the sole consequence of individual judicial appraisal, is predetermined by the human programmer and the dataset provided by him or her.

However, judicial independence means that the decision-making process is not interfered with and not that it is unrelated to data on which it is based. A human judge is (even more so than algorithms, perhaps) "programmed" by his/her knowledge of law, available information (in practice, this nowadays amounts to electronic databases of case law and of scholarly works), cultural and social background, individual prejudices, etc. Independence entails personal and institutional qualities required for impartial decision-making, and it is thus a prerequisite for impartiality.[13] It characterises both a state of mind which denotes a judge's imperviousness to external pressure as a matter of moral integrity, and a set of institutional and operational arrangements which must provide safeguards against undue influence and/or unfettered discretion of the other State powers.[14] This makes independence a characteristic of a tribunal's relations vis-à-vis the other branches of government[15] and the parties to the proceedings[16]. What matters is that there must be no external, undue influence from the outside on how justice is administered in a particular case. Even the political nature (or "flavour") of the judicial appointment process as such does not necessarily mean that the requirement of independence is always impaired[17] – provided that sufficient safeguards exist protecting the sterile judicial decision-making mechanism. Taking into account the concerns regarding the independence of AI judges from the possible undue influence of other branches of government[18], one cannot but note that from a normative perspective they are no different from those concerning any other undue influence on judicial decision-making. The difference lies in the technological implementation of such influence, but not in the influence itself.

Obviously, specific technical safeguards are required to protect the algorithm from external influence while deciding cases. Yet, theoretically, achieving the required standard of independence is not excluded when algorithms are used for adjudicating purposes. The same conclusion applies to the requirement concerning the way in which a court is established. As the CJEU rightly held in *A.K. v. Krajowa Rada Sądownictwa*:

> "although the principle of the separation of powers between the executive and the judiciary has assumed growing importance in its case-law, neither Article 6 nor any other provision of the ECHR requires States to adopt a particular constitutional model governing in one way or another the relationship and interaction between the various branches of the State, nor requires those States to comply with any theoretical constitutional concepts regarding the permissible limits of such interaction. The question is always *whether, in a given case, the requirements of the ECHR have been met*".[19]

It follows that while there may be different methods of appointing judges, they can entail different degrees of political involvement. Ultimately, however, it comes down to an overall assessment of whether the judicial branch is sufficiently protected from the undue political influence by government, as is also the case for the independence requirement.

Therefore, while relying on AI as a judge clearly raises serious concerns pertaining to the requirement of independ-

ence, it appears that these concerns are no more pertinent than in the case of human judges. In a way the opposite might be true – AI promises more transparency in the sense that anyone (obviously provided they have enough technical expertise) can actually check the dataset on which AI judgments are based, whereas no one can consult the mind of a human judge.

2. Fairness

If sufficient technological safeguards exist – which by nature is more a technical than a legal question – that protect the independence of AI judiciary (understood as immunity from undue influence from other branches of government), the question nevertheless remains whether an AI judge is able to ensure *fairness* as a precondition of the right to a fair trial.

The right to a fair trial does not necessarily need to encompass a right to substantive fairness (a "proper" judgment). In some jurisdictions, it extends to a substantive fairness guarantee[20], in others it does not[21]. In the European constitutional space, the notion of a "fair trial" is limited to the question of procedural fairness, i.e. whether the rule of law is respected and therefore the adjudication was free of arbitrariness.[22] From the point of view of the ECHR, it thus constitutes a "purely procedural guarantee".[23]

Nonetheless, *fairness* represents one of the constructional requirements of the right to a fair trial, being "one of the fundamental principles of any democratic society".[24] It presupposes that claims and observations of either party are *duly considered* by a trial court.[25] *Fairness* places "the *tribunal* under a duty to conduct a *proper examination* of the submissions, arguments and evidence adduced by the parties, without prejudice to its assessment of whether they are relevant to its decision".[26] The requirement of *fairness* encompasses a number of detailed conditions such as equality of arms,[27] adversarial trial,[28] reasoning of rulings,[29] freedom from self-incrimination,[30] lawfulness of administration of evidence,[31] or the principle of immediacy[32]. But *fairness* is much more than just observing procedural rules – it is about *properly* considering the material of a case at hand and about avoiding any arbitrariness in its judicial appraisal. *Fairness*, in that way, also seems to be substantively interlinked with the right to *effectiveness* of judicial protection, since the latter is unlikely to be respected if the former is not.

So, can we have a *fair* trial, i.e. *proper examination* of the case pending before a court, if this court is an AI one? This leads us to the question of how we should understand *proper examination* (or *due consideration*), and whether or not this could be upheld without a human component.

II. On the Notion of "Proper Examination (Due Consideration)" and Why We (Sometimes) Need Human Judges

European Court of Human Rights (ECtHR) case law has been consistent in its stance that "the right to a fair trial cannot be seen as effective unless the requests and observations of the parties are truly 'heard', that is to say, properly examined by the tribunal".[33] This means that the court is "under a duty to conduct a proper examination of the submissions, arguments and evidence adduced by the parties, without prejudice to its assessment of whether they are relevant to its decision".[34] This duty is not limited to providing sufficient reasoning of the tribunal's decisions,[35] but extends to due consideration of the body of evidence collected before it.

The "due consideration" requirement entails proper in-depth examination of the body of evidence produced before a tribunal. For instance, in criminal cases "a conviction ignoring key evidence constitutes a miscarriage of criminal justice".[36] One must note that properly assessing the gravity of evidence and its significance for the proper examination of a case requires very complex analyses. These do not necessarily need to follow the pre-existing patterns according to which an AI judge would come to a decision. Every single case constitutes a more or less unique bundle of factual findings and "due consideration" requires assessing their individual relevance for the ruling as well as judicial appreciation of their interconnections. This results in a duty to address sometimes very complex factual backgrounds of cases where different elements are mutually interlinked.

In *Farzaliyev v. Azerbaijan*, for example, the ECtHR reproached national courts for failing to provide sufficient reasoning behind their fact-finding. Yet it seems quite clear that what the courts were really failing to do was to respond to the abusive institution of criminal proceedings for the sole purpose of reviving a claim period when all the statutes of limitations had long expired. While the ECtHR criticism primarily/ostensibly targeted the lack of reasoning, the real issue was the abuse of the law in its application *in fraudem legis*.[37] Similarly, in *Cupiał v. Poland*, the national courts – in the Court's view – not only failed to respond to the applicant's allegations, but moreover "no efforts were made to *analyse* this issue".[38] The assertions and pleas forwarded by a party to a court trial must

be "carefully considered" (*"soigneusement examinés"* in French) and analysed "thoroughly and seriously" (*"approfondi et sérieux"* in French), which under the fair trial guarantee is considered a separate requirement from providing a proper reasoning.[39]

However, "due consideration" also requires properly subjecting a tribunal's decision to the scrutiny of social reality and the present-day conditions. As aptly pointed out by *Jordi Nieva-Fenoll*, laws

> "must adapt to the times, or end up sending Galileo Galilei to the fire, and for this the work of the judge is essential. In their mission to analyse the specific situation in which the rule is to be applied, they must observe the nuances of that situation and determine the best application for it. While this makes the application of the law less predictable than what a mathematician would accept or what an AI programmer would imagine, it is precisely what will guarantee that the law does not enter as a foreign body into people's lives, but reasonably regulates their coexistence".[40]

In light of this, "duly considering" a case appears to be the antithesis of "dully considering" it. It goes far beyond simply applying the law, thus presupposing application of justice. The former cannot be achieved without also taking into consideration ("duly considering" vs. "dully considering") different social contexts and changing attitudes of a given society. What would have been perceived as just when a law was adopted might be considered appalling when it is applied – or, as the Grand Chamber held in *Fedotova and others v. Russia,* "what may have been regarded as *permissible and normal* at the time when the Convention was drafted may subsequently prove to be incompatible with it".[41]

Artificial intelligence, in its current state of development, is capable of analysing (probably much more thoroughly and precisely than humans) very complex data and subsuming a legal norm deduced from the legal system to an established factual situation. But that's really all it can do. So what is missing? Three observations can be made in this regard.

Firstly, as matters stand, AI seems unable to develop an interpretation of the law that adequately takes into account the ever-changing social landscapes surrounding the processes of "doing justice." Ignoring this obstacle and pressing ahead with AI-driven judgment risks an algorithm applying the law correctly from a strictly formal point of view, yet completely missing the mark when it comes to the societal sense of fairness and justice (the risk of an overly positivistic AI judge). This sense of fairness and justice relies heavily on perceptions of various societal phenomena. Let us take the example of "socially acceptable criticism and exaggeration" as a concept that comes into play when competing interests are weighed against each other, – in this case the right to respect for personal dignity vs. freedom of expression. On numerous occasions, the ECtHR has been confronted with complaints about the judicial application of national laws limiting freedom of expression in cases of "exaggerated" criticism. It has become consistent case law of the Court that national authorities are under a duty to assess whether the "generally accepted limits of exaggeration" were exceeded.[42] So far, it seems unlikely that an an AI judge would be able to appreciate the subtleties of a particular expression in a way that would ensure these accepted limits are adhered to. . This would require a very nuanced knowledge of what is accepted by the general public, while taking into account various current social developments. It should be noted that when the ECtHR scrutinises the proportionality of state interventions (even when the classic elements of a proportionality review – i.e. adequacy, reasonability, and necessity – are not explicitly referred to by the Court[43]), it assesses the measures applied against the legitimate aims pursued, and takes into account what is perceived to be fair and just in a process of judicial appreciation.

Secondly, defining a norm deduced from the provisions of a given legal system, while considering not only its provisions but also scholarly writings and the jurisprudence, seems a task perfectly tailored to artificial intelligence. After all, it involves the analysis of complex databases, which are closed sets of data with a predetermined scope. Yet appraising the body of evidence is something inherently different because evidence may vary according to factual circumstances. In turn, these factual circumstances cannot reasonably be predetermined in most cases (except maybe for relatively simple cases of unpaid invoices, etc.). Again, falling back on AI when deciding cases that present more complicated evidence may compromise the duty – rooted in the right to a fair trial – to carefully, thoroughly, and seriously analyse particular pieces of evidence and their interconnections against the general background of a case. The assessment of evidence, as a whole, must be "fair and proper",[44] and this remains a task that many humans are unable to accomplish, let alone artificial intelligence.

Thirdly, as things stand, AI justice appears unsuitable as a classic branch of government. The primary role of the judiciary is, of course, to decide individual cases and apply justice. However, administration of justice goes way beyond specific cases. It is also a part of the checks and balances formula characterising modern democratic societies. As a consequence, the judiciary's interpretations sometimes need to be more extensive when the political

branches of the government plainly fail to respond to society's needs, or when these political branches turn dysfunctional. Judging when the time has come for the judiciary to quickly respond to state failure or dysfunctional government (or, conversely, when it should demonstrate more self-restraint) entails careful consideration of very complex socio-political processes and, almost physically "feeling" them. Given AI's reliance on predetermined and available definitions and datasets, this seems still unachievable for an AI judiciary.

III. Conclusions

The use of artificial intelligence as a tool for judicial decision-making is becoming ever more widespread. It goes hand in hand with the idea of replacing human judges with AI. While the use of AI as a judge would largely benefit the efficiency and predictability of the administration of justice, its use would be neutral when it comes to fair-trial criteria such as the right to professional legal representation or legal aid. When it comes to independence and impartiality, AI judges appear no more likely to fall of short of these requirements than human judges, provided that sufficient technical safeguards are in place.

Nonetheless, the use of AI (in its current state of development) as judges does not seem to be reconcilable with the right to "fairness" of a court trial, which includes the duty of the trial court to duly consider the case.

For one, this is because more complicated litigations implying complex analysis of the body of evidence and the interconnections between particular pieces of evidence against a general factual background seem to exceed the technical scope of AI as envisaged by developers. What is more, AI seems equally unable to duly consider concepts which require human intuition, without which justice cannot be administered fairly (i.e. corresponding to the general sense of what is fair and just). Lastly, AI does not seem to be able to genuinely play the role of the judicial branch of State powers maintaining checks and balances on the political branches. It does not seem to be capable of navigating the interpretation of the law in such a way as to properly respond to possible failures and dysfunctions of the legislative and the executive branches (i.e. sometimes applying more dynamic interpretation, other times being more self-restrained).

It follows that in cases that are more complicated than simply ordering payment on the basis of outstanding and undisputed invoices, the use of AI in the judiciary system may compromise the requirement of fairness, which is one of the commonly accepted definitional elements of the right to a fair trial. Instead of "duly considering" such cases, AI – predetermined and limited by the underlying dataset – is likely to "dully consider" them.

Marcin Górski
Professor of the Department of European Constitutional Law, University of Łódź. Member of the Migration Law Research Centre of the Polish Academy of Sciences.

1 M. Szwast, *Kształtowanie się prawa do sądu w prawie polskim przed uchwaleniem Konstytucji RP z 1997 r.*, Przegląd Konstytucyjny 2019, no. 3, pp. 33–60.
2 C. Teleki, *Due Process and Fair Trial in EU Competition Law The Impact of Article 6 of the European Convention on Human Rights*, Leiden-Boston, Brill/Nijhoff 2021, pp. 74–75 and the scholarly works cited therein.
3 ECtHR (GC), *Guðmundur Andri Ástráðsson v. Iceland*, 1.12.2020, appl. no. 26374/18, § 233.
4 See e.g. Articles 15, 18 and 121 of the Dutch Constitution (*Grondwet voor het Koninkrijk der Nederlanden),* Article 36 of the Czech Charter of Fundamental Rights and Freedoms (*Listina základních práv a svobod*), Article 9 of the Swedish Instrument of Government (*Kungörelse (1974:152) om beslutad ny regeringsform*), Sections 119, 241, 1171, and 1201 of the Spanish Constitution (*Constitutión Española*), Article 23 of the Slovenian Constitution (*Ustava Republike Slovenije*), Articles 46–48 of the Slovak Constitution (*Ústava Slovenskej republiky*), Articles 21 and 24 of the Romanian Constitution (*Constituția României*), Articles 20 and 203 of the Portuguese Constitution (*Constituição da República Portuguesa*), Article 45 of the Polish Constitution (*Konstytucja Rzeczypospolitej Polskiej*), Articles 24, 104, and 111 of the Italian Constitution (*Constituzione della Repubblica Italiana*), Article 7 of the French Declaration of Human and Civic Rights (*Declaration des Droits de l'Homme et du Citoyen*), or Articles 19, 97, 101 and 103 of the German Basic Law (*Grund-gesetz für die Bundesrepublik Deutschland*).
5 E. S. Corwin, "Debt of American Constitutional Law to Natural Law Concepts", (1950) 25 *Notre Dame L. Rev.,* 258–284, 275.
6 ECtHR (plenary), *Sutter v. Switzerland,* 22.02.1984, appl. no. 8209/78, at § 27.
7 See F. Palmiotto, "Preserving Procedural Fairness in The AI Era. The Role of Courts Before and After the AI Act", *verfassungsblog.de*, 5.01.2023, <https://verfassungsblog.de/procedural-fairness-ai/> accessed 23 February 2023; J. E. Baker, L. N. Hobart, and M. G. Mittelsteadt, "AI for Judges. A Framework". *CSET Policy Brief,* December 2021 <https://www.armfor.uscourts.gov/ConfHandout/2022ConfHandout/Baker2021DecCenterForSecurityAndEmergingTechnology1.pdf> accessed 26 April 2023.
8 P. M. Nowotko, "AI in judicial application of law and the right to a court", (2021) 192 *Procedia Computer Science*, 2220–2228, 2224.

9 G. Gentile, "AI in the courtroom and judicial independence: An EU perspective", *EUIdeas,* 22.08.2022,<https://euideas.eui.eu/2022/08/22/ai-in-the-courtroom-and-judicial-independence-an-eu-perspective/> accessed 13 March 2023.
10 European Commission, "Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", 21.04.2021, COM(2021) 206 final 2021/0106(COD).
11 C.A. Severance, "The Constitution and Individualism", (1922) vol. 8, no. 9 *American Bar Association Journal*, 535–542.
12 I. Brownlie, "The Place of the Individual in International Law", (1964) Apr., vol. 50, no. 3, *Virginia Law Review,* 435–462; J. Klabbers, "The Individual in International Law", in: J. Klabbers (ed.), *International Law*, 2013, pp. 107–123.
13 ECtHR, *Dolińska-Ficek and Ozimek v. Poland,* 8.11.2021, appl. nos. 49868/19 and 57511/19, at § 316.
14 ECtHR (GC), *Guðmundur Andri Ástráðsson v. Iceland*, cited above, at § 234.
15 ECtHR, *Beaumartin v. France,* 24.11.1994, appl. no. 15287/89, at § 38.
16 ECtHR (plenary), *Sramek v. Austria,* 22.10.1984, appl. no. 8790/79, at § 42.
17 ECtHR, *Salicor Lormine v. France,* 9.11.2006, appl. no. 65411/01, at § 67.
18 See e.g. T. Sourdin, "Judges, Technology and Judicial Independence", in: T. Sourdin (ed.), *Judges, Technology and Artificial Intelligence. The Artificial Judge,* Edgar Elgar Publ. 2021, pp. 189–208.
19 CJEU, 19.11.2019, Joined Cases C585/18, C624/18 and C625/18, *A.K. v. Krajowa Rada Sądownictwa,* § 130.
20 See e.g. the Constitutional Court of South Africa, 5.04.1995, *S v Zuma and Others,* 1995(2)SA 642(CC), where Justice Kentridge held that "The right to a fair trial conferred by that provision is broader than the list of specific rights […]. It embraces a concept of substantive fairness".
21 See e.g. ECtHR (GC), *García Ruiz v. Spain*, 21.01.1999, appl. no. 30544/96, at § 29.
22 ECtHR (GC), *Al-Dulimi and Montana Management Inc. v. Switzerland*, 21.06.2016, appl. no. 5809/08, at § 145.
23 L. Garlicki, P. Hofmański, and A. Wróbel, *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*, C.H. Beck, Warsaw 2010, comments on Article 6 ECHR, item 159.
24 ECtHR (plenary), *Pretto v. Italy,* 8.12.1983, appl. no. 7984/77, at § 21.
25 ECtHR, *Donadze v. Georgia,* 7.03.2006, appl. no. 74644/01, at § 35.
26 ECtHR, *Kraska v. Switzerland,* 19.04.1993, appl. no. 13942/88, at § 30.
27 ECtHR (GC), *Öcalan v. Turkey,* 12.05.2005, appl. no. 46221/99, at § 140.
28 ECtHR (GC), *Rowe and Davis v. the United Kingdom,* 16.02.2000, appl. no. 28901/95, at § 60.
29 ECtHR (GC), *Moreira Ferreira v. Portugal (No. 2),* 11.07.2017, appl. no. 19867/12, at § 84.
30 ECtHR, *Funke v. France,* 25.02.1993, appl. no. 10828/84, at § 44.
31 ECtHR, *Ayetullah Ay v. Turkey,* 27.10.2020, appl.nos. 29084/07 and 1191/08, at §§ 123–130.
32 ECtHR, *Cutean v. Romania,* 2.12.2014, appl. no. 53150/12, at § 61.
33 ECtHR, *Dulaurans v. France,* 21.03.2000, appl. no. 34553/97, at § 33; *Carmel Saliba v. Malta,* 29.11.2016, appl. no. 24221/13, at §65; *Cupiał v. Poland,* 9.03.2023, appl. no. 67414/11, at § 56.
34 ECtHR, *Van den Hurk v. the Netherlands,* 19.04.1994, appl. no. 16034/90, at § 59.
35 ECtHR, *Ajdarić v. Croatia,* 13.12.2011, appl. no. 20883/09, at § 34.
36 ECtHR (GC), *Moreira Ferreira v. Portugal (No. 2),* 11.07.2017, appl. no. 19867/12, at § 63.
37 ECtHR, *Farzaliyev v. Azerbaijan,* 28.05.2020, appl. No. 29620/07, at §§ 34–40.
38 ECtHR, *Cupiał v. Poland,* 9.03.2023, *op. cit.* (n. 33), at § 63.
39 ECtHR, *Donadzé v. Georgia,* 7.03.2006, appl. no. 74644/01, at §§ 32 and 35; ECtHR, *Dima v. Romania,* 16.11.2006, appl. no. 58472/00, at § 34.
40 J. Nieva-Fenoll, "Technology and fundamental rights in the judicial process", (2022) vol. 13, no. 2 *Civil Procedure Review,* 60.
41 ECtHR (GC), *Fedotova and others v. Russia,* 17.01.2023, appl. nos. 40792/10, 30538/14 and 43439/14, at § 170, while invoking the ECtHR (plenary), *Marckx v. Belgium*, 13.06.1979, appl. 6833/74, at § 41 (concerning discrimination of "illegitimate" children).
42 ECtHR, *Kurski v. Poland*, 5.07.2016, appl. no. 26115/10, § 54, *Kharlamov v. Russia*, 8.10.2015, appl. no. 27447/07, § 32, *Ciorhan v. Romania*, 3.12.2019, appl. no. 49379/13, § 34, *Monica Macovei v. Romania*, 28.07.2020, appl. no. 53028/14, §§ 92–93, *Steel i Morris v. the United Kingdom*, 15.02.2005, appl. no. 68416/01, § 90.
43 J. Gerards, "How to improve the necessity test of the European Court of Human Rights", (2013) vol. 11, no. 2 *I•CON*, 466–490, at 467–468.
44 ECtHR (GC), *Blokhin v. Russia,* 23.03.2016, appl. no. 47152/06, at § 202.

"Legalize It!?" – Opportunities and Challenges for the Regulation of Cannabis under European Law

Is Legalisation Legal?

Oliver Landwehr and Daniel-Erasmus Khan*

Following similar developments in other parts of the world (e.g. Uruguay, Canada, United States, Thailand), several countries in the EU are questioning or openly challenging the prohibitionist paradigm that has so far dominated international drug control law. Possibly the most far-reaching approach is contained in the concept paper *(Eckpunktepapier)* adopted by the German Federal Government in October 2022, which would provide for the comprehensive regulation of cannabis for recreational use from "seed to sale". While the legality of this approach under public international and EU law has been called into question, this article shows that a responsible regulation of cannabis is not only desirable from a policy perspective but also legally feasible.

I. Background

On 26 October 2022, the German government adopted key principles for the controlled sale of cannabis to adults for recreational purposes.[1] Following up on their bold promise in the Coalition Agreement, according to which the three parties forming the current government "will introduce the controlled sale of cannabis to adults for recreational purposes in licensed shops,"[2] the concept paper outlines how the production, supply, and distribution of recreational cannabis would be authorised within a licensed and state-controlled framework. This effort aims to strengthen harm reduction[3], improve the protection of minors and the health of consumers, and curtail the black market. While the proposal enjoys broad support in society and was welcomed by civil society organisations active in the field of harm reduction, it has also encountered resistance from conservative parties and critical voices in the legal literature, who question its legality. This is not surprising as the German plans go beyond any existing efforts to decriminalise or regulate cannabis in the European Union (EU). At the same time, the German plans represent the only consistent and comprehensive model in the EU, and possibly even in the world. Therefore, the issue whether they are compatible with existing EU law deserves attention. Before turning to that question, however, we will first briefly present the international drug control regime, and analyse why it has failed and possibly done more harm than good.

1. The international drug control regime

There can be no doubt that drugs[4] are dangerous. As the virtually universal Single Convention on Narcotic Drugs of 1961[5] (the Single Convention) reminds us in its preamble, "addiction to narcotic drugs constitutes a serious evil for the individual and is fraught with social and economic danger to mankind." Yet the preamble also recognises that "the medical use of narcotic drugs continues to be indispensable for the relief of pain and suffering." Moreover, humans have been using some form of mind-altering substances throughout the history of humankind.[6] Against this backdrop, it hardly comes as a surprise that two (opposing) paradigms have dominated drug control regimes over the last century: prohibition and regulation. Historically, the USA has been a champion of prohibition, while producing,[7] manufacturing,[8] and consuming states (led by Turkey, the United Kingdom, and other European countries) have been favouring a regulatory approach.[9] More recently, however, these roles seem to have been partly reversed.

a) A brief history of drug control[10]

Over the past two centuries, the answer to the crucial question how to deal with drugs has always been closely linked to both economic interests and general developments in the political-societal sphere. In the mid-18th century, when France and Britain twice used military force in the Far East, they did *not* do so in order to fight the drug trade but rather to open up the Chinese market for opium, particularly originating from India. The notorious "Opium Wars"[11] forced China to end the enforcement of its prohibition against opium trafficking by British merchants and to legalise the opium trade. It is safe to assume that these conflicts, along with various treaties imposed during the "century of humiliation", caused a national trauma that still resurfaces during present-day discussions about cannabis legalisation by Western countries and helps to explain China's visceral opposition to any such plans.

It was not until 1907 that Britain, China, and India agreed on a trilateral framework for ending Indian opium exports to China within ten years.[12] Two years later, the Shanghai Opium Commission was initiated under US leadership as the first multilateral drug control meeting to examine ways of suppressing international opium traffic, and in particular traffic bound for China. While the meeting only made recommendations, it led to the 1912 Hague Opium Convention, the first international drug control treaty.[13] In 1925, the Geneva Opium Convention[14] established the first mechanisms to enforce a supply control framework. It created the Permanent Central Opium Board (PCOB), one of the forerunners of today's International Narcotics Control Board (**INCB**)[15], to monitor international imports and exports of narcotics. Further conventions were adopted in 1931 and 1936. Repeatedly, the United States tried but failed in all these negotiations to obtain a ban on all "non-medical and non-scientific" drug use. This approach must also be seen against the backdrop of alcohol prohibition in the United States, where the Eighteenth Amendment to the Constitution was ratified by the requisite number of states in early 1919, prohibiting the production, importation, transportation, and sale of alcoholic beverages from 1920 until it was repealed in 1933.

After World War II, the United Nations (UN) became the custodian of the existing treaties. In 1946, a functional commission of the UN Economic and Social Council (ECOSOC), the Commission on Narcotic Drugs (**CND**), was set up to serve as the policy-making body of the UN system with prime responsibility for drug-related matters. In 1948, the Synthetics Protocol brought synthetic narcotics under international control for the first time. The United States again tried to impose more severe limitations on the agricultural production of opiates through the 1953 Opium Protocol. However, as it was rejected by agricultural producing and consumer countries, as well as moderate states, it never entered into force. Instead, the **1961 Single Convention on Narcotic Drugs** consolidated previous conventions into one document (hence the name). It applies to opioids, coca, and cannabis. As countries with important pharmaceutical industries refused to extend the scope of the Single Convention to psychotropic substances, a separate convention was negotiated. The **1971 Convention on Psychotropic Substances**[16] (the 1971 Convention) brings psychotropic substances[17] under international control, but is less stringent than the Single Convention.[18]

From the early 1970s onwards, the United States stepped up its supply-side targeting drug policies again. In June 1971, in a speech to the White House Press Corps, US President Richard Nixon declared a "war on drugs". Although the restrictive, prohibitionist, and supply-side focussed US approach on drug policy dates back much longer, this speech is often seen as the beginning of a counter-productive and systemically racist domestic and international crusade that lasted several decades.[19] The focus on trafficking also led to the adoption of the **1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances**[20] (the 1988 Convention), which aims at tackling organised crime and drug trafficking. It also introduced extensive precursor[21] controls.

These legal instruments were complemented by an institutional framework and non-binding resolutions and declarations. In 1972, a UN Fund for Drug Abuse Control (UNFDAC) was created. The Fund and the United Nations Drug Control Programme later merged with the Crime Fund and the Centre for International Crime Prevention to form what is today the United Nations Office on Drugs and Crime (**UNODC**), an organisational unit of the UN Secretariat headquartered in Vienna, Austria. UNODC also acts as the Secretariat to the CND and hosts its annual sessions. In the 1990s, the UN General Assembly also turned its attention to the topic. At a UN General Assembly Special Session (**UNGASS**) in 1998, states committed to massive reductions in drug use and supply within ten years and coined the slogan, "A drug free world. We can do it!" Almost 20 years later, the third UNGASS in 2016 was more realistic and marked a break with traditional "war on drugs" approaches, even though it failed to break with the prohibitionist paradigm.[22]

Nevertheless, since the 1990s, a new paradigm in drug policy has emerged that recognises that there will always be some people who will use drugs, and some people who may be unwilling or unable to stop using drugs. This concept, called "**harm reduction**", therefore promotes policies, programmes, and practices that aim to minimise the negative health, social, and legal impacts associated with drug use, drug policies, and drug laws. Harm reduction focusses on positive change, and on working with people who use drugs without judgement, coercion, discrimination, or requiring that they stop using drugs as a precondition of support. It is cost-effective, evidence-based, and human rights-centred. Examples of harm reduction measures are needle and syringe exchange programmes, opioid agonist therapy (such as methadone), drug checking (where drugs are checked for adulterants), and drug consumption rooms to reduce the risk of fatal overdose.

b) The international drug control conventions

As countless resolutions of the CND remind us, three UN conventions form the "cornerstone" of the international drug control regime: the 1961 Single Convention, the 1971 Convention on Psychotropic Substances, and the 1988 Anti-trafficking Convention (the Conventions).[23] None of these Conventions contains a comprehensive and unconditional

obligation for states to impose criminal sanctions on (all forms of) drug possession and/or use.

- The 1961 Single Convention obliges its parties to limit exclusively to medical and scientific purposes the production, manufacture, export, import, distribution of, trade in, use, and possession of drugs (Art. 4(c)). Drugs are defined as the substances listed in "schedules" to the Convention (Art. 1(j)).[24] Cannabis and cannabis resin, extracts, and tinctures are listed in Schedule I.[25] Art. 36(1)(a) contains penal provisions which obliges any party, "subject to its constitutional limitations," to make certain actions, including the possession of drugs, punishable offences. However, subpara. (b) allows for alternatives to conviction or punishment when "abusers"[26] of drugs have committed such offences. It is also important to note that Art. 36 does not refer to "use."[27] Therefore, the possession for personal use is also considered to be outside the scope of the provision.[28]
- The 1971 Convention contains essentially the same limitations of drug use and penal provisions (Art. 5 and 22). Even though cannabis as such was already regulated in the Single Convention, its psychoactive ingredient, tetrahydrocannabinol (THC), is contained in Schedule I of the 1971 Convention only, as it was not yet known to science at the time the Single Convention was adopted.
- The 1988 Convention goes one step further than the previous conventions in that its Art. 3(2) requires parties to establish as a criminal offence the possession, purchase, or cultivation of drugs "for personal consumption" as well. This obligation, however, is subject to each party's "constitutional principles and the basic concepts of its legal system."[29] Moreover, para. 4(c) of this provision provides for alternatives to conviction or punishment "in appropriate cases of a minor nature." This effectively removes the obligation to criminalise possession for personal use. In fact, in its 2021 Annual Report, the INCB explicitly acknowledges that "measures to decriminalize the personal use and possession of small quantities of drugs are consistent with the provisions of the drug control conventions."[30] If personal use and possession can be decriminalised, a strong argument can be made that necessary precursor acts committed in the framework of a regulatory system are also consistent with the Conventions.

If **decriminalisation** is in line with the Conventions, then **depenalisation**[31] must, *a fortiori*, also be possible. By contrast, the INCB takes the view that **legalisation**, i.e. legislation implementing "policies that explicitly permit the non-medical and non-scientific use of internationally controlled substances" and entailing no penalty whatsoever, is in violation of the international drug control conventions.[32] While this view is shared by many conservative states, it must be borne in mind that the Conventions are inherently flexible. A case in point is decriminalisation itself: Not so long ago, the INCB held the view that decriminalisation was not in line with the Conventions, and even considered harm reduction measures like drug consumption rooms as inadmissible. In this context, it should be born in mind that, in the absence of a court that could provide an authentic interpretation of the Conventions, their meaning is defined by the parties, and there is no one single valid interpretation.[33] Lastly, the INCB (which seems to use the terms legalisation and regulation interchangeably[34]) ignores that regulation is a concept that is fully in line with the object and purpose of the Conventions to improve the "health and welfare of mankind," reduce the "public health and social problems" resulting from drug use, prevent addiction, and combat the illicit production of and traffic in drugs.[35]

c) EU drug law

Drugs are mentioned only twice in the Treaty on the Functioning of the European Union (**TFEU**): Art. 83(1) provides a legal basis for the adoption of directives to establish minimum rules concerning the definition of criminal offences and sanctions for certain "areas of particularly serious crime with a cross-border dimension," which include "illicit drug trafficking." Art. 168(1) stipulates that the Union shall complement the Member States' action in reducing drugs-related health damage, including information and prevention.

Secondary legislation on the issue is scarce as well: Under the Lisbon Treaty (on the basis of Art. 83(1) TFEU), just one drug-related directive has been adopted so far.[36] It amends the definition of "drug" in **Framework Decision** 2004/757/JHA.[37] This Framework Decision (FD), which was adopted in the third pillar under the former Nice Treaty, lays down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking. In this respect, Art. 2 of the FD provides that:

> 1. Each Member State shall take the necessary measures to ensure that the following intentional conduct when committed without right is punishable:
>
> (a) the production, manufacture, extraction, preparation, offering, offering for sale, distribution, sale, delivery on any terms whatsoever, brokerage, dispatch, dispatch in transit, transport, importation or exportation of drugs;
>
> (b) the cultivation of opium poppy, coca bush or cannabis plant;
>
> (c) the possession or purchase of drugs with a view to conducting one of the activities listed in (a);
>
> (d) the manufacture, transport or distribution of precursors, knowing that they are to be used in or for the illicit production or manufacture of drugs.
>
> 2. The conduct described in paragraph 1 shall not be included in the scope of this Framework Decision when it is commit-

ted by its perpetrators exclusively for their own personal consumption as defined by national law.

Apart from the FD, there is little legislation that is relevant to the question of cannabis regulation. An earlier Joint Action[38] has been repealed and has not been incorporated in the FD. The Schengen *acquis* deals with narcotic drugs in Title III, Chapter 6 of the Convention Implementing the *Schengen* Agreement (CISA) . These provisions are mostly concerned with the import and export of drugs, including cannabis. Art. 71(2) obliges the contracting parties to undertake to "prevent and punish by administrative and penal measures the illegal export of narcotic drugs and psychotropic substances, including cannabis, as well as the sale, supply, and handing over of such products and substances".

The Council also regularly adopts decisions on the position to be taken, on behalf of the European Union, at the sessions of the CND, with regard to the vote on the scheduling recommendations from the World Health Organisation (WHO).[39] In particular, in December 2020, the CND voted on a re-scheduling of cannabis and cannabis-related substances. The Council decision supported the WHO recommendation to delete cannabis and cannabis resin from Schedule IV of the Single Convention.[40]

In addition to legislation, however, soft law also needs to be considered. Most relevant in the current context are the **EU drugs strategies** that have been approved by the Council, and the corresponding action plans. The most recent versions of the EU drugs strategy and action plan cover the period 2021 to 2025.[41] Importantly, they do not require EU Member States to criminalise drug use. On the contrary, the strategy notes that "drug consumption and/or drug possession for personal use or possession of small amounts do not constitute a criminal offence in many Member States, or there is the option to refrain from imposing criminal sanctions."[42] **Council conclusions** of March 2018 promote the use of alternatives to coercive sanctions for drug using offenders.[43] In 2022, the Council approved conclusions on a human rights-based approach in drug policies acknowledging that, in line with the 2018 Council conclusions, the term "alternatives to coercive sanctions" could, according to national legislation of the EU Member States, also refer to alternatives that are used instead of or alongside the traditional criminal justice measures for drug-using offenders.[44]

2. The problems with prohibition

a) Prohibition is not working

It can hardly be denied that the existing drug control regime has had little effect: For years, both the supply and the demand of controlled drugs have been constantly rising.[45]

In principle, there are two possible responses to this finding: First, one can claim that without this regime, the situation would be even worse and that therefore, we just have to enforce it even stricter. In the absence of a counterfactual, this argument can never be entirely disproved. However, it is implausible for many reasons. Firstly, very strict, even extreme, supply-side and law enforcement-centred approaches have been tried for decades. As mentioned above, the United States even declared a "war on drugs" from the 1970s onwards. This "war" has not been won, on the contrary. Secondly, as UNODC noted in its first Transnational Organized Crime Threat Assessment, since transnational organised crime is driven by market forces, countermeasures must disrupt those markets, and not just the criminal groups that exploit them.[46] The enforcement approach neglects the demand side and ignores the fact that wherever there is a demand that cannot be satisfied legally, be it for drugs or anything else, an illicit market will appear.[47] As long as that illicit market generates profits, it will not disappear. Thirdly, in the face of extreme drug crises, countries have been forced in the past to change tack and adopt a more health- and harm reduction-oriented approach. This was the case in Portugal in the 1990s and can be seen today in the United States, where – faced with an opioid epidemic that currently claims over 100,000 drug deaths per year – the Biden administration has issued a new drug control strategy that clearly embraces harm reduction measures for the first time.[48] Fourthly, cutting off the drug supply, e.g. for millions of opioid addicts in the United States, would not cure them of their addiction, nor address the root causes of the epidemic. Lastly, it is not clear whether consumption would rise in the absence of prohibition. While this seems intuitive, the evidence is inconclusive.[49] Even a rise in consumption, however, does not necessarily entail more harm: The purity and quality of licit cannabis is clearly superior to substances sold in the streets; drug-related crime and imprisonment would decrease; and risk awareness raising and protection of minors (e.g. ID checking) could be carried out more effectively.

Therefore, the second and more convincing response would be to admit that the existing regime is not working and needs to be changed. A radical approach would be to scrap the system entirely. This, however, is neither practical nor desirable for a number of reasons, not least because it would jeopardise the supply security of controlled medicines. Rather, a strictly regulated licit market should replace an uncontrolled illicit market. It is debatable whether this is preferable for all drugs. In the case of alcohol, the experiment with prohibition in the United States at the beginning of the last century clearly demonstrated the advantages of a regulated market over an unregulated criminal one. The increasingly strict regulation of tobacco has been a success story, with cigarette use, especially among young people, in sharp decline over the last two

decades. Cannabis is the logical candidate to test this strategy in the field of currently controlled substances.

b) Prohibition is harmful

Prohibition is not only not working, it is also positively harmful. Addiction – or rather 'drug use disorder' – can be a form of sickness.[50] It is not helpful to criminalise sick people. Criminalisation creates stigma, marginalisation and discrimination, and raises structural barriers for people who wish to access service such as drug treatment and harm reduction as they fear punishment.

As noted above, prohibition has created an illicit market that will not disappear as long as it generates profits. These illicit markets are feeding organised crime groups that have grown into horrendous proportions. Some of these cartels have become so powerful that they resemble quasi-states. The result is crime and bloodshed at an unprecedented scale, massive corruption, state capture, and failed or failing states. The war on drugs has cost thousands of lives and has destabilised entire countries.[51] Some countries are also taking lives through the imposition of the death penalty for drug-related offences and extrajudicial killings. Prison overcrowding has become a massive problem, especially in the United States.

Yet, there is no way to win the "war on drugs" by military or law enforcement means. The only way to put the cartels and organised crime groups out of business is to deprive them of their income. This would effectively destroy them and can only be achieved by regulating access to drugs. This approach also minimises the harm done by drugs, with both unregulated illicit and unregulated licit markets causing the greatest harm. A regulated market presents the best opportunity for reducing that harm.

Finally, from an economic perspective, current drug policy – especially with regard to cannabis – is a waste of money[52], a waste of time, and a waste of human resources. As you can only spend available financial resources once, it should be spent on those interventions that are the most effective in terms of health protection and harm reduction. This analysis applies, in principle, to all licit and illicit drugs, but regulation must be tailored to each drug. There can be no one-size-fits-all approach. This article only deals with the regulation of cannabis.

3. The winds of change

Despite the evidence that the current regime of prohibition is not working and has significant negative or "unintended" consequences, the legal straightjacket of the three above-mentioned UN Conventions has kept change very slow and uneven.

a) Drug reform and cannabis regulation outside the EU

In 2013, **Uruguay** became the first country in the world to legalise the recreational adult use of cannabis for its citizens and residents. In 2015, **Jamaica** introduced a decriminalisation model of cannabis use in order to divert users from the criminal justice system. This was followed by **Canada** in 2017, which has allowed its citizens and residents to acquire quality-controlled cannabis through legal supply chains. The country has also developed comprehensive harm reduction services.

In 2018, the Constitutional Court of **South Africa** ruled that the use and possession of cannabis, and the cultivation of cannabis plants by an adult for personal consumption in private no longer constitute criminal offences. Likewise, in **Mexico**, the supreme court ruled the criminalisation of cannabis use unconstitutional.

In 2019, **Thailand** was the first country in the region to legalise medical uses of cannabis before fully de-scheduling it from its Narcotics Act in 2022. In 2019, **New Zealand** introduced a decriminalisation model allowing for law enforcement discretion towards personal drug use and possession. However, in New Zealand, a narrow majority rejected a model of adult cannabis legalisation by referendum in 2020.

In 2021, **Switzerland** passed the legal framework for the regulated sale of cannabis. This has enabled cantons, municipalities, universities, and other organisations to conduct pilot studies to gain scientific knowledge about alternative approaches to regulating the non-medical use of cannabis.

In the **United States**, the use and sale of cannabis continue to be illegal at the federal level. However, to date, 21 jurisdictions (18 states, two territories, and the District of Columbia) have legalised the use of cannabis for non-medical purposes, while 37 states permit medical use. In 2022, the Biden administration announced a review of the scheduling status of cannabis. This process could lead to federal regulation of sales for recreational use. US President Biden also signed a law to ease onerous restrictions on cannabis research, and to grant pardons to offenders convicted for cannabis use and possession.[53]

b) Developments in EU Member States

Portugal was the first country in the EU to decriminalise all drug use. Due to the pressure from the three UN Conventions, however, it remains an administrative offence.

The **Netherlands** has a long-standing policy of tolerating the sale of cannabis for personal use in coffee shops, which have been able to sell small quantities of cannabis for personal consumption since 1970. However, as the cultivation and sale of cannabis is not permitted, coffee shops have had to obtain their cannabis from illegal sources. In 2020, the Netherlands therefore introduced legal production of cannabis as an experimental pilot project in ten cities.

In 2021, **Luxembourg** announced the legalisation of adult cannabis use and cultivation (a maximum of four plants) within home settings. The same year, **Malta** passed a law on "responsible use of cannabis." This law allows adults to possess up to 7 g of cannabis, domestic cultivation of up to four cannabis plants, and the storage of up to 50 g of dried cannabis product. In addition, people can form non-profit organisations for the purpose of cultivating cannabis exclusively for the organisation's members within the framework of a risk and harm reduction approach.

As outlined above, **Germany** plans to comprehensively regulate cannabis from seed to sale. **Czechia** has announced similar plans.

II. The Compliance of Cannabis Regulation with EU Law

When it comes to the "if and how" of regulating cannabis in their domestic legal sphere, countries outside the EU have little to fear from the international legal order. This is true even for those states who have opted for a comprehensive regulation model like in Canada, which might not be in compliance with the three Conventions.[54] Indeed, the Conventions lack effective enforcement mechanisms, and the CND in particular does not dispose of any such mechanisms. Apart from issuing statements, the utmost the INCB could do is to recommend to parties that they impose a drugs embargo on the country concerned.[55] In practice, this has never happened and is unlikely to happen in the future.[56] For EU Member States, however, the situation is quite different: Their domestic policy choices are, in addition to obligations under general international law, effectively limited by EU law, an enforceable legal regime.

1. The 2004 Framework Decision on illicit drug trafficking

As mentioned earlier,[57] conduct related to self-consumption of cannabis does not fall within the scope of FD 2004/757/JHA laying down minimum rules in regard to drug trafficking offences and penalties. Recent reforms in Luxembourg and Malta are therefore *ab initio* not affected by the FD. The more far-reaching models in the Netherlands and in Germany, however, are *prima facie*[58] not limited to conduct by persons for their own personal consumption. Instead, what is at stake here is a regulation of the entire distribution chain "from seed to sale". Hence, the question arises whether this is in compliance with the FD.

An initial and paramount observation in this respect is the wording of the title of the FD: It was adopted to counter criminal acts "in the field of illicit drug trafficking." Likewise, Art. 2 FD relates to "crimes linked to trafficking."

The proposed German licence model is of course the very opposite of illicit drug trafficking. Qualifying the cultivation and sale of cannabis through a strictly regulated state-licensed system as "illicit drug trafficking" would turn the meaning of these terms on its head. To any non-lawyer, this would seem so obvious and clear that it does not require any further explanation. Conversely, lawyers are well known for their creativity in interpreting legal norms. However, at least in the realm of criminal law, a cardinal principle exists which is deeply rooted in the *Rechtsstaatsprinzip* (rule of law), namely that the natural meaning of words marks the outer limits of their interpretation.[59] Qualifying the state-regulated acts in question as "trafficking" would clearly overstep these limits.

This is also important insofar as the EU does not have a general criminal law competence to legislate on drugs, but only one regarding "illicit drug trafficking" (Art. 83 (1) TFEU). Although the 2004 FD predates this norm, which was introduced by the 2009 Lisbon Treaty, its identical wording must be interpreted in strict conformity with the EU Treaties. Holding otherwise would lead to the untenable result of a criminalisation of conduct for which the EU has no competence.

These considerations are confirmed by the explicit caveat that limits Art. 2 FD to acts "committed without right." Conduct carried out on the basis of an act of parliament, and under a state-issued licence can hardly be considered "without right."

An interpretation that respects the natural meaning of terms should stop here. However, for the sake of the argument, we will also explore if this conclusion could be challenged if the words "illicit trafficking" and "without right" were to be understood as a reference to international drug control law.

a) Licensed conduct is not "committed without right"

Unlike the "personal use" clause in Art. 2(2) FD 2004, the "without right" clause in Art. 2(1) does not explicitly and

necessarily refer to national law. Moreover, all EU Member States are also parties to the three UN Conventions. Some authors therefore seem to assume that "states can only recognise a 'right' under the clause if this does not violate their obligations under international law."[60] This view, however, has no basis in the text of the FD and completely ignores the autonomy of EU law.

In that respect, it must be noted that the FD does not incorporate the international drug control regime into Union law. On the contrary, its preamble does not even once mention the three UN Conventions. The only place these Conventions are referred to is in the definition of "drugs" and "precursors" in Art. 1 FD. Therefore, the words "without right" must be given an autonomous interpretation.

The clause in Art. 2(1) FD grants Member States a possible derogation from the mandatory criminalisation. Any limitation of that derogation must be interpreted restrictively: first because we are in the field of criminal law (and limiting the "rights" expands criminalisation); and second because the TFEU strictly limits the Union's competence to the criminalisation of acts related to "trafficking." Finally, the interpretation must also preserve the *effet utile* of the clause.

Applying these principles, it must be noted that it would have been easy for the drafters of the FD to include a reference to international law in the chapeau of Art. 2(1). Instead of, or in addition to the words "without right," they could simply have used the term "illicit conduct" and defined it elsewhere as "not in compliance with the international drug control conventions." In order to enhance legal certainty, they could also have incorporated the essence of the Conventions into the FD by criminalising conduct "when committed for non-medical and non-scientific purposes." Yet, they chose the unusual wording "without right." It must thus have an independent meaning going beyond these cases.

In other words, to require that any "right" under this clause must be in conformity with the Conventions would limit the meaning of the clause to medical and scientific use – as these are the only permitted uses under the UN Conventions. Therefore, equating the clause with "right in conformity with the Conventions" would deny it any independent meaning going beyond illegality under international law. The caveat "without right" would thus have no *effet utile*. It follows that these words must mean that illegality under international law is a necessary – *but not sufficient* – condition for punishment.

Indeed, the ordinary meaning of the words "without right" does not simply mean "illegally," but rather without authorisation. This would seem to result even clearer from some other language versions of Art. 2(1) FD.[61] It is further supported by the meaning of the clause in two other EU instruments harmonising criminal law where it is used (in the English version[62]): In both Directive 2011/92/EU and Directive 2013/40/EU, the words "without right" are explicitly defined as referring (also) to a permission or an authorisation under domestic law.[63] The fact that in Directive 2011/92/EU and Directive 2013/40/EU the clause is given a defined meaning also contradicts the view that "without right" implies a limitation to medical and scientific use. If that were the case, it would certainly have been included in the definitions in Art. 1 or in the Preamble of the FD.

It is therefore more convincing to interpret the clause in Art. 2(2) FD 2004 as a reference to a national authorisation. A licence system would constitute such an authorisation.

Lastly, the fact that the Member States are parties to the three UN Conventions, and the EU to the 1988 Convention, does not change this conclusion. The EU competence under the 1988 Convention is explicitly limited to precursor control. Therefore, cannabis regulation is outside the EU competence. Moreover, the status of international law in the domestic legal order is determined by the domestic legal order. Countries that follow the monist theory may be prevented from establishing a licence system to authorise and regulate cannabis cultivation and use because they might see themselves bound by the international Conventions. This does not, however, apply to countries that follow the dualist theory. Even if they were in breach of international obligations (which is debatable, see below), this would have no consequence for the validity of the domestic legislation. Since the landmark judgment in *Kadi*[64], we know that EU law does not follow a (purely) monist system. Illegality under international law does not automatically entail illegality under EU law. In any case, the EU would have no competence to issue an authorisation. Therefore, any reference in the FD 2004 must be a reference to national law.

b) Licensed conduct does not constitute "illicit trafficking"

The term "illicit trafficking" is a pleonasm: There is no such thing as "licit" trafficking. Trafficking is inherently unlawful.[65] If a state decides to responsibly regulate a drug rather than leave it to the unregulated illicit market, it does not engage in trafficking. Any assertion to the contrary would contravene the meaning of "trafficking." This must of course be distinguished from a hypothetical situation in which a "rogue" state, e.g. a failed state under the control of a narco cartel, actively engages in activities that are illegal under its own laws or decides to turn a blind eye. This could indeed

be called state trafficking but is very different from the situation in question.

This argument does not only apply to the FD but also to the three Conventions. In reality, a state regulation model as the one planned in Germany lies outside the scope of the Conventions because, like the FD, they are limited to illicit trafficking. They were never meant to apply to a state-controlled distribution system.

It must also be called to mind that it is not easy to decide what constitutes "illicit" behaviour under the UN Conventions. Given the great flexibility of the Conventions, which is regularly invoked by all parties, the interpretation of what is in line with the Conventions is not easy and has changed dramatically over time.[66] In the absence of an authoritative interpretation of the Conventions[67], each state is free to make that assessment for its own conduct. As noted above, states' (and the INCB/CND's) assessment is liable to change over time as well.[68]

c) Licensed conduct benefits from the exemption in Art. 2(2) FD

All of the above rests on the premise that the "personal consumption" exemption in Art. 2(2) FD is not applicable to the situation in question. If it were, state-licensed regulation of cannabis would fall outside the scope of the FD entirely. Indeed, there are very good reasons to substantiate this case.

Art. 2(2) FD does not only cover the possession and use but all the acts in para. 1 that necessarily precede consumption. It is true that the exemption is limited to conduct committed by its perpetrators for their own personal consumption. However, if preparatory conduct is exempted when carried out by users then, *a fortiori*, that conduct must be exempted if it is carried out under a state-issued licence. The FD simply did not foresee such a situation. Nevertheless, it would be highly inconsequential and illogical if state-regulated conduct were to be treated less favourably than the same conduct by a consumer. Moreover, that conduct (cultivation, distribution etc.) is a *necessary* precursor to the later consumption. Lastly, para. 2 clarifies that "personal consumption" is defined by national law. Arguably, that law therefore remains free to include in "personal consumption" all acts that necessarily precede the final consumption.

2. The Schengen acquis

As mentioned above, the Schengen acquis is primarily concerned with trans-border situations, and deals with the import and export of narcotic drugs. Importantly, a Joint Declaration has effectively modified Art. 71(2) CISA.[69] This Joint Declaration allows contracting parties, under certain conditions, to depart from the principle referred to in Art. 71(2). As a consequence, the creation of a national licensing system for recreational adult-use cannabis would not be in breach of the Schengen acquis as long as the regulatory model aims to contribute to the prevention of addiction, and provided that administrative and penal measures are taken to prevent and punish cross-border illegal drug trafficking.[70] All of this would be fulfilled under the German model.

3. CJEU jurisprudence

National drug policy is a highly political area that – given its relevance for health protection, criminal law, and law enforcement – touches the core of national sovereignty. Therefore, the European Commission would probably hesitate to second-guess national choices in this matter and refrain from instituting infringement proceedings against a Member State (Art. 258 TFEU). Nevertheless, bearing in mind that infringement actions can also be brought by other Member States (Art. 259 TFEU), the question of interpretation of the 2004 FD on illicit drug trafficking may eventually reach the Court of Justice of the European Union (CJEU) as the final arbiter of EU law.

How the Court would approach such a case is anyone's guess. That said, the case law leaves room for optimism. In particular, the CJEU's seminal CBD case[71] is inspiring. In a judgment concerning the free movement of goods, the judges in Luxembourg examined the question whether cannabidiol (CBD) is covered by the Single Convention. They could have chosen an easy route, as they found "that a literal interpretation of the provisions of the Single Convention might lead to the conclusion that, in so far as CBD is extracted from a plant of the Cannabis genus and that plant is used in its entirety – including its flowering or fruiting tops – it constitutes a cannabis extract […] and, consequently, a 'drug' within the meaning […] of that convention."[72]

Instead, the Court made the effort to carry out a teleological interpretation and held that "since CBD does not contain a psychoactive ingredient in the current state of scientific knowledge […], it would be contrary to the purpose and general spirit of the Single Convention to include it under the definition of 'drugs' within the meaning of that convention as a cannabis extract."[73] The Court therefore concluded that CBD is not a "drug" within the meaning of the Single Convention.[74] This indicates that the CJEU is prepared to consider the purpose of the Conventions to protect the "health and welfare of mankind," and reduce "public health and social problems" when interpreting them. *A fortiori*, this must be borne in mind when interpreting Union law.

Ultimately, the Court will have to apply the Charter of Fundamental Rights of the European Union when interpreting the 2004 FD and the CISA. The right to privacy in Art. 8 of the Charter could provide a powerful basis for a judgment in favour of a responsible cannabis legalisation. In this case, the Charter would take primacy over treaty law.[75] The *Kadi* jurisprudence has set a strong precedent in this respect.[76] There are very good reasons why this case law, which gives priority to the protection of fundamental rights over international obligations, should also be applied in the present context.

III. Conclusion

In her foreword to the 2021 Report of the Global Commission on Drug Policy, *Helen Clark* notes:

> "[i]n general, the world looks to international law to support the achievement of humanity's fundamental aspirations, including of human rights for all. Yet in drug policy, international law itself bears much of the responsibility for the world's failure to address drug use in a rational and humane way."[77]

Unfortunately, there is little hope that this will change any time soon. Given the extremely divergent approaches to drug policy among the state parties to the three UN Conventions on drug control, amending these Conventions is all but impossible in the foreseeable future. In all likelihood, the global drug control regime will thus remain stuck in the 1960s forever. This makes it all the more important not to interpret Union law as condemning EU Member States to perpetuate the errors of the past. This article has sought to demonstrate that, correctly interpreted, Union law does in fact not stand in the way of responsible regulation at the national level. Nature and scope of the German Federal Government's proposed regulation of cannabis constitute such a regime.

Dr. Oliver Landwehr, LL.M. Eur
Counsellor UNODC matters, Delegation of the European Union to the International Organisations in Vienna

Prof. Dr. Daniel-Erasmus Khan
Professur für Öffentliches Recht, Europarecht und Völkerrecht, Universität der Bundeswehr, Munich

* The views expressed in this article are those of the authors and do not necessarily reflect the official opinion of the European Union institutions.

1 Bundesgesundheitsministerium, "Eckpunktepapier der Bundesregierung zur Einführung einer kontrollierten Abgabe von Cannabis an Erwachsene zu Genusszwecken". See press release: <https://www.bundesgesundheitsministerium.de/ministerium/meldungen/kontrollierte-abgabe-von-cannabis-eckpunktepapier-der-bundesregierung-liegt-vor.html> accessed 15 January 2023.

2 "Mehr Fortschritt Wagen - Bündnis Für Freiheit, Gerechtigkeit Und Nachhaltigkeit", Koalitionsvertrag 2021–2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), p. 68.

3 On this term, see below I.1.a) *in fine*.

4 The term "drugs" is generally used to mean narcotic and psychotropic substances. However, non-controlled substances like alcohol and nicotine are also drugs in the wider sense and at least as harmful.

5 UNTS, vol. 976, No. 14152. 186 states are parties to the 1961 Convention (as amended by the 1972 Protocol).

6 Cf. only (with further references) M.-A. Crocque, "Historical and Cultural Aspects of man's relationship with addictive drugs", (2007) *Dialogues in Clinical Neuroscience*, 355–361.

7 Countries cultivating poppy, coca leaf, and cannabis.

8 Countries with pharmaceutical industries.

9 Scholars have noted that "the Single Convention represented a victory for the regulatory strand and UK-led coalitions over the US-led prohibitionist strand," cf. J. Collins, *Legalising the drug wars: a regulatory history of UN drug control*, 2021, p. 224.

10 This short overview draws heavily on the detailed account in two seminal books: J. Collins, *Legalising the Drug Wars: a regulatory history of UN drug control*, 2021; and W. B. McAllister, *Drug Diplomacy in the Twentieth Century*, 1999.

11 "Opium Wars" is a collective term for the conflicts between Western powers and China, including the First Opium War (UK vs. China, 1839–1842), and the Second Opium War (UK & France vs. China,1856–1860).

12 See R. K. Newman, "India and the Anglo-Chinese Opium Agreements, 1907–1914", (1989) *Modern Asian Studies*, 525–560.

13 League of Nations Treaty Series, vol. 8, pp. 188–239.

14 League of Nations Treaty Series, vol. 81, pp. 318–358.

15 The INCB styles itself as a quasi-judicial body tasked with monitoring the compliance with the international drug control conventions. This seems to be based on Art. 14 of the Single Convention, on Art. 19 of the 1971 Convention, and on Art. 22 of the 1988 Convention. However, these articles do not, in fact, contain such a broad mandate. As a last resort, the INCB can recommend to parties that they stop the import of drugs, the export of drugs, or both, from or to the country concerned ("embargo").

16 UNTS, vol. 1019, No. 14956.

17 Psychoactive drugs such as amphetamine-type stimulants, barbiturates, benzodiazepines, and psychedelics.

18 For instance, the threshold to schedule a substance under the 1971 Conventions is higher (two thirds) than for the Single Convention (simple majority).

19 See also J. Hari, *Chasing the Scream. The Search for the Truth About Addiction*, 2015.
20 UNTS, vol. 1582, No. 27627.
21 Precursors are (licit) substances frequently used in the illicit manufacture of drugs (cf. Art. 12 of the 1988 Convention).
22 The Outcome Document of the 2016 UNGASS is widely considered to be the most progressive negotiated UN drug policy document to date.
23 For a succinct overview, see N. Boister, "The international legal regulation of drug production, distribution and consumption", (1996) vol. 29 *The Comparative and International Law Journal of Southern Africa*, 1–15.
24 The term "illicit drugs", although it is frequently used in CND resolutions (presumably to distinguish them from "licit" drugs like alcohol and tobacco), is not used in the Conventions. Therefore, it is preferable to speak of controlled substances.
25 Cannabis and cannabis resin also used to be in Schedule IV, which comprises the most harmful drugs (cf. Art. 3(5) of the Single Convention). After a long and very controversial discussion, the CND decided (by a very close vote) in 2020 to de-schedule cannabis from Schedule IV. It remains listed in Schedule I.
26 The terms "abuse" and "abuser" are nowadays considered stigmatising and should be avoided.
27 The 1973 Commentary on the Single Convention on Narcotic Drugs (Prepared by the Secretary-General in accordance with para. 1 of ECOSOC resolution 914 D (XXXIV)) notes that "article 36 is intended to fight the illicit traffic, and unauthorized consumption of drugs by addicts does not constitute 'illicit traffic'" (Art. 36, para. 7).
28 The Commentary (note 27) on Art. 36 (para. 8) refers to Art. 4, where it is noted that the purpose ("to fight the illicit traffic") and the *travaux préparatoires* of the Single Convention "support the opinion of those who believe that only possession for distribution, and not that for personal consumption, is a punishable offence under article 36" (para. 18; also Art. 33, para. 2).
29 In 1993, upon ratification of the 1988 Convention, Germany made an interpretative declaration on Art. 3(2), stating that the caveat ("subject to … the basic concepts of its legal system") can change over time: "It is the understanding of the Federal Republic of Germany that the basic concepts of the legal system referred to in article 3, paragraph 2 of the Convention may be subject to change." This means that the country can now argue that in the meantime, harm reduction has become a basic concept of its legal system, and that the intended regulation of cannabis is grounded in harm reduction and health protection. To that end, Germany can cite evidence that the prohibition of cannabis has not led to a reduction of cannabis (on the contrary, use is increasing), and that THC content has increased, making the sale of unregulated cannabis products increasingly dangerous.
30 Para. 380.
31 According to the INCB, depenalisation describes "a situation in which the behaviour in question remains a criminal offence but in which there is a reduction of the use of existing criminal sanctions, which does not require changes to the law, as in the case of decriminalization."
32 INCB, *2021 Annual Report*, paras. 375–376.
33 On the mandate of the INCB, cf. note 15.
34 In our view, the term "legalisation" should be avoided because it could imply a complete absence of regulation.
35 Cf. below I.2.
36 Directive (EU) 2017/2103 of the European Parliament and of the Council of 15 November 2017 amending Council Framework Decision 2004/757/JHA in order to include new psychoactive substances in the definition of "drug," and repealing Council Decision 2005/387/JHA, *O.J.* L 305, 21.11.2017, p. 12.
37 Council Framework Decision 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking, *O.J.* L 335, 11.11.2004, 8 (amendments: *O.J.* L 305, 21.11.2017, 12; L 66, 7.3.2019, 3; L 379, 13.11.2020, 55; L 178, 20.5.2021, 1; L 200, 29.7.2022, 148). According to its Art. 1, "'drugs': shall mean any of the substances covered by the following United Nations Conventions: (a) the 1961 Single Convention on Narcotic Drugs (as amended by the 1972 Protocol); (b) the 1971 Vienna Convention on Psychotropic Substances. It shall also include the substances subject to controls under Joint Action 97/396/JHA of 16 June 1997 concerning the information exchange risk assessment and the control of new synthetic drugs."
38 Joint Action 96/750/JHA of 17 December 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the approximation of the laws and practices of the Member States of the European Union to combat drug addiction and to prevent and combat illegal drug trafficking, *O.J.* L 342, 31.12.1996, 6.
39 These decisions are based on Art. 83(1), in conjunction with Art. 218(9) TFEU.
40 Council Decision (EU) 2021/3 of 23 November 2020 on the position to be taken, on behalf of the European Union, at the reconvened sixty-third session of the Commission on Narcotic Drugs, on the scheduling of cannabis and cannabis-related substances under the Single Convention on Narcotic Drugs of 1961, as amended by the 1972 Protocol, and the Convention on Psychotropic Substances of 1971, *O.J.* L 4, 7.1.2021, 1. The Decision was adopted with a qualified majority and is binding on Member States. Despite this, Hungary voted against the Union position at the CND. The Commission therefore initiated an infringement procedure in February 2021. On 15 February 2023, the Commission referred the case to the Court of Justice.
41 EU Drugs Strategy 2021–2025, 18 December 2020, Council Doc. 14178/20; EU Drugs Action Plan 2021–2025, *O.J.* C 272, 8.7.2021, 2.
42 Para. 7.4.
43 Council doc. 6931/18.
44 Council doc. 15818/22, 8 December 2022, p. 6.
45 For instance, the estimated number of people who use drugs has risen from 185,000 in 1998 to 269,000 in 2018 (International Drug Policy Consortium, *Taking Stock: A Decade of Drug Policy*). The global illicit production of opium has increased by 950% since 1980. On cannabis consumption, cf. also UNODC, *World Drug Report 2022*, Booklet 3, p. 3 *et seq*.
46 UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*, 2010, p. iii.
47 The size of that illegal market is estimated to amount to USD 500bn, controlled by transnational organised crime groups.
48 Office of National Drug Control Policy, *2022 National Drug Control Strategy*, p. 30 *et seq.*; cf. already previously Office of National Drug Control Policy, *Biden-Harris Administration's Statement of Drug Policy Priorities for Year One*, 2021.
49 The experience in the USA would suggest a rise, both with regard to alcohol (after the end of prohibition in 1933), and cannabis. In Canada, however, the data is not so clear. Moreover, unlike in the USA, in Canada, the perception that cannabis can be addictive has increased, especially among people who use cannabis regularly (UNODC, *2022 World Drug Report*, Booklet 3, p. 23, fig. 19).
50 UNODC and WHO generally refer to 'drug use disorders' rather than 'addiction'. See the International Treatment Standards for the Treatment of Drug Use Disorders, https://www.who.int/publications/i/item/international-standards-for-the-treatment-of-drug-use-disorders. They also note that "8% of individuals who start using psychoactive drugs will develop a drug use disorder over time, with significant variations for different classes of psychoactive substances" (p. 4). So the great majority of people who use drugs do so without developing a 'disorder'.

51 In 2019, 36,661 people were killed in drug-related violence in Mexico alone, according to the Instituto Nacional de Estadistica y Geografia.
52 An estimated USD 100bn is spent annually on the war on drugs (Global Commission on Drug Policy, *Time to End Prohibition*, p. 16).
53 Cf. <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/06/granting-pardon-for-the-offense-of-simple-possession-of-marijuana/; https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/06/statement-from-president-biden-on-marijuana-reform/> accessed 15 January 2023.
54 This is, however, debatable, see above I.1.b) and below II.1.b).
55 Cf. note 15.
56 If only because the work of the INCB is largely funded by the US. In any case, such a recommendation would be non-binding.
57 Cf. I.1.c).
58 But see below c).
59 Cf. only recently, German Federal Constitutional Court, Order of 5 May 2021 (2 BvR 2023/20 et al.), mn. 13.
60 Cf. P. H. van Kempen/M. Fedorova, *Cannabis regulation through the "without rights"-clause in Article 2(1) of EU Framework Decision 2004/757/JHA on illicit drug trafficking*, 2022, p. 14.
61 In French: "ne peuvent être légitimés", in German: "ohne entsprechende Berechtigung". The term "Berechtigung" clearly points to a positive authorisation rather than a mere illegality under international law.
62 In other language versions, the terms used in the 2004 FD and in the mentioned two instruments is not always identical (e.g. in French: "sans droit"; in German: "unrechtmäßig" and "unbefugt").
63 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *O.J.* L 335, 17.12.2011, 1 (Art. 5 and the definition in para. 17 of the Preamble); Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *O.J.* L 218, 14.8.2013, 8 (Art. 2(d)).
64 CJEU, 3 September 2008, Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission*, ECLI:EU:C:2008:461.
65 According to the Cambridge Dictionary, trafficking is the "activity of buying and selling goods or people illegally."
66 See above 1.b).
67 The INCB does not have a treaty mandate to monitor the implementation of the Convention, although it claims to be a quasi-judicial body with such powers, cf. above note 15. The three Conventions contain clauses on dispute settlement by the ICJ. However, this has never happened and many parties have made reservations on these provisions (e.g. Art. 48(2) and 50 of the Single Convention).
68 Cf. the interpretative note by Germany, quoted above in note 29.
69 Joint Declaration included in the Final Act of the CISA.
70 This view is shared by van Kempen/Fedorova, op. cit. (n. 55), p. 11–12.
71 CJEU, 19 November 2020, Case C-663/18, *Commercialisation du cannabidiol (CBD)*, ECLI:EU:C:2020:938.
72 Para.71 of the judgment.
73 Para. 75 of the judgment.
74 Para. 76 of the judgment.
75 D. Thym, "Ein Weg zur Cannabis-Legalisierung führt über Luxemburg", *Verfassungsblog*, <https://verfassungsblog.de/ein-weg-zur-cannabis-legalisierung-fuhrt-uber-luxemburg/>. Also see the articles on *Verfassungsblog* by K. Ambos (https://verfassungsblog.de/zur-volkerrechtlichen-zulassigkeit-der-cannabis-entkriminalisierung/) and R. Hofmann (<https://verfassungsblog.de/cannabis-2/>). All accessed 15 January 2023.
76 See supra note 59 and for a detailed analysis K. Ziegler, "The Relationship between EU Law and International Law", in D. Patterson and A. Södersten (eds.), *Blackwell Companion for European Union Law and International Law*, 2016, pp. 42–61.
77 Global Commission on Drug Policy, *Time to End Prohibition*, 2021. Helen Clark is a former Prime Minister of New Zealand and has been Chair of the Global Commission since 2020.

Limitations of the Transnational *ne bis in idem* Principle in EU Law

Remarks on the ECJ's Diesel Scandal Volkswagen Case

Laura Neumann

The *ne bis in idem* principle is one of the most fundamental guarantees in criminal procedure law. It prohibits a second prosecution in cases that have already been concluded by a final decision. According to the traditional understanding, the principle excludes a duplication of proceedings only within the same jurisdiction. Art. 50 CFR, however, which was incorporated into primary EU law by Art. 6 TEU, extends the principle's scope to the transnational sphere to the effect that a final decision in one Member State constitutes a bar to new proceedings in other Member States of the EU as well. While this transnational *ne bis in idem* guarantee in principle allows for limitations, these must meet the requirements provided for by Art. 52 para. 1 CFR.

The pending Case C-27/22, which has its roots in the diesel scandal involving German automobile producer Volkswagen, gives the Court of Justice of the European Union an opportunity to set new standards in this regard, which might be of high relevance for the future understanding of the *ne bis in idem* guarantee in a single area of freedom, security, and justice. In particular, it offers the Court the chance to provide guidance on the conditions that an EU secondary law provision must meet in order to be qualified a legitimate legal basis for a limitation to the transnational *ne bis in idem* principle. Furthermore, it gives the Court the opportunity to clarify whether all of the specifications of the criteria for limitations to the intra-state *ne bis in idem* guarantee that have been developed in *Menci and Garlsson Real Estate,* and were elaborated in *BV* and *bpost* also apply at inter-state level.

This article sheds light on these questions by discussing the criteria for limitations of the *ne bis in idem* principle, including their specifications originally established for intra-state cases, against the background of the Volkswagen Case C-27/22, which is transnationally structured.

I. Previous Relevant Case Law

To date, the Court of Justice of the European Union (ECJ) has recognised two kinds of limitations of the *ne bis in idem* guarantee as meeting the conditions set out by Art. 52 para. 1 CFR.

The first group of cases concerns limitations based on the Convention implementing the Schengen Agreement (CISA), which is a *sui generis* act of EU law of the same hierarchical order as secondary Union law.[1] In the *Spasic* judgment, the ECJ acknowledged that the enforcement condition enshrined in Art. 54 CISA constitutes a limitation of the individual right granted by Art. 50 CFR within the meaning of Art. 52 para. 1 CFR.[2] Furthermore, in *MR*, decided on 23 March 2023, the Court also recognised Art. 55 para. 1 lit. b) CISA as a valid limitation of the fundamental right guaranteed by Art. 50 CFR.[3]

A second group of cases concerns possible justifications for limitations of the intra-state *ne bis in idem* guarantee provided for by national legislation. In this regard, the ECJ made important specifications to the criteria set out in Art. 52 para. 1 CFR in *Menci*[4] and *Garlsson Real Estate*[5], which it further elaborated in *BV*[6] and in the *bpost* case[7]. These specifications will be discussed in detail in Section III.

The pending Case C-27/22 (*Volkswagen Group Italia and Volkswagen Aktiengesellschaft*) neither concerns an exception to the inter-state *ne bis in idem* guarantee based on the CISA nor an exception to the intra-state *ne bis in idem* principle based on provisions of national law. Instead, it deals with a possible limitation of the inter-state *ne bis in idem* guarantee which echoes the first group of cases but is based on a provision of regular EU secondary legislation contained in a directive, rather than the CISA. This notably raises two questions: First, what prerequisites apply for a regular EU secondary law provision to serve as a legal basis for a limitation to the *ne bis in idem* principle under Art. 52 para. 1 CFR? Second, to what extent may the specific conditions developed in *Menci* and *Garlsson Real Estate*, and further elaborated in *BV* and *bpost*, be transferred to inter-state level?

It should be noted that the *Nordzucker* case[8], decided on 22 March 2022, related to possible limitations of the transnational *ne bis in idem* guarantee as well. It does, however, concern the special area of competition law that has been harmonised in the EU to the point of allowing it to be treated nearly like a harmonious national system.[9] Therefore, *Nordzucker* is not predictive of the present case.

II. Case C-27/22: Facts, Procedure and Preliminary Questions Referred to the ECJ

In Case C-27/22, the ECJ is called to give a preliminary ruling on questions that arose in Italian administrative proceedings in the context of the diesel scandal.[10] The starting point of the dispute was a fine of € 5 million imposed on Volkswagen AG (VWAG) and Volkswagen Group Italy (VWGI) by the Italian Antitrust Authority (AGCM) on 4 August 2016 for an infringement of the Italian Consumer Code. The alleged infringement concerns the marketing of vehicles with manipulated systems for the measurement of pollutant emissions in Italy and advertisements emphasising the compliance of said vehicles with the Italian environmental regulatory criteria. VWGI and VWAG appealed against the decision. In 2018, while the appeal in Italy was still pending, the German public prosecutor's office of Braunschweig, Lower Saxony, imposed an administrative fine of € 1 billion on VWAG (based on the German Act on Regulatory Offenses (*Ordnungswidrigkeitengesetz*)) for essentially the same facts as alleged by the Italian proceedings; however, the reasoning concerned VWAG's entire global marketing – including in Italy – instead of the Italian marketing only. Both the Italian and the German authorities ordered the maximum fine provided for by the respective national legislation. While the German fine order became final in June 2018, the Italian appeal is still pending before the *Consiglio di Stato*. It was this court that lodged a request for preliminary ruling to the ECJ.

The Italian court's request is three-fold: For one, it aims to find out whether the penalties imposed for unfair commercial practices under Italian law implementing Directive 2005/29/EC[11] can be classified as *criminal* administrative penalties and, therewith, trigger the applicability of the *ne bis in idem* principle. In light of the ECtHR's and the ECJ's case law,[12] this question will presumably be answered in the affirmative.

A second question raised by the Italian court makes reference to the specific chronological order of the steps of the two proceedings. In particular, this question concerns the fact that while the Italian administrative penalty was imposed before the German penalty, a final decision has been made on the latter, whereas the appeal against the Italian penalty is still pending.[13] Prior case law of the ECJ and the ECtHR in this context, at least as far as intra-state constellations are concerned, indicates that the applicability of the *ne bis in idem* principle does not depend on a specific order of the steps of the proceedings in question, but rather requires any proceedings to be concluded whenever a decision concerning the same offence in the material sense becomes final.[14] There is no apparent reason why this should be different in a transnational setting.

The third and final question raised by the Italian court concerns the issue of possible limitations to the transnational *ne bis in idem* guarantee. Specifically, the referring court aims to find out whether the provisions laid down in Art. 3 para. 4 and Art. 13 para. 2 lit. e) of Directive 2005/29/EC justify a derogation from the *ne bis in idem* guarantee established by Art. 50 CFR and Art. 54 CISA. This question will be discussed in more detail in the following section.

III. Requirements for Limitations of the *ne bis in idem* Principle and Specifications in Intra-State Cases

In the relevant case law regarding possible justifications of limitations of the *ne bis in idem* principle at intra-state level, the ECJ has been consistently structuring its analyses the same way.

The judges in Luxembourg start off by reemphasising that, according to the *Spasic* judgment, a limitation of the *ne bis in idem* principle guaranteed by Art. 50 CFR may be justified on the basis of Art. 52 para. 1 CFR.[15] This is followed by a detailed analysis of the individual criteria of Art. 52 para. 1 CFR and their application to the respective case.

According to the first sentence of Art. 52 para. 1 CFR, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. The second sentence further provides that any limitations are subject to the principle of proportionality and may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

In accordance with the analyses regularly performed by the Court, Art. 52 para. 1 CFR may be broken down into five criteria. First, the limitation in question must be provided for by law. Second, it must respect the essence of the rights and freedoms it limits. Third, it has to meet an objective of general interest. Fourth, it must comply with the principle of proportionality. Fifth, it must be strictly necessary in order to achieve the objective of general interest it serves.

With regard to the first requirement (that any limitation on the exercise of fundamental rights, such as the one enshrined in Art. 50 CFR, must be provided for by law), the ECJ made it clear in *BV*[16] and reiterated in *MR*[17] that the legal basis which permits restricting a fundamental right must in turn define the scope of this limitation. It follows that, according to the Court, the first requirement is broadly indissociable from the requirements of clarity and precision arising from the principle of proportionality. Accordingly, the clarity and preciseness of the rules establishing the limitation to the *ne bis in idem* guarantee, which the Court had identified as a sub-criterion of the requirement of strict necessity in *Menci*[18] and *Garlsson Real Estate*[19], is in fact a precondition in itself for those rules to be qualified as a legal basis for a limitation of Art. 50 CFR in the first place. Consequently, the respective law must establish rules clear and precise enough to allow individuals to predict which acts or omissions could give rise to a duplication of proceedings and penalties to meet the "provided for by law" criterion.[20]

On a similar note concerning the second criterion of respecting the essence of Art. 50 CFR, the ECJ regards a clear and comprehensive definition of the conditions that would lead to a duplication of proceedings and penalties as a precondition for ensuring that the right guaranteed by Art. 50 CFR is not called into question as such.[21] Whenever rules do not clearly, precisely, and exhaustively define the prerequisites for a limitation of the *ne bis in idem* principle, they leave room for abuse and at least carry the risk of the essence of Art. 50 CFR being brought into question per se.

Regarding the third criterion (requiring an objective of general interest to be served by the limitation of the *ne bis in idem* guarantee), the ECJ established in *Menci* and *Garlsson Real Estate* that, for the purposes of meeting such an objective of general interest, a duplication of criminal proceedings and

penalties may be justified where they pursue complementary aims relating to, as the case may be, different aspects of the same unlawful conduct in question.[22] In *bpost*, the Court identified such a pursuit of complementary objectives by the different proceedings as a factor of relevance for the proportionality requirement as well and made it clear that this factor could justify the additional burden resulting from the cumulation of the different procedures and penalties.[23]

With regard to the principle of proportionality as such, which constitutes the fourth criterion set out by Art. 52 para. 1 CFR, the ECJ regularly provides a general explanation that the duplication of proceedings and penalties may not exceed what is appropriate and necessary in order to attain the legitimate objectives at issue. According to the Court, it goes without saying that given several appropriate measures, recourse must be had to the least onerous one, and that the disadvantages caused must not be disproportionate to the aims pursued.[24]

As far as the fifth and final criterion is concerned, the rules allowing for the duplication of proceedings and penalties have to be strictly necessary to achieve the objective of general interest. In this context, the Court made three important specifications in *Menci* and *Garlsson Real Estate*.[25] Firstly, it stated that the legislation limiting the *ne bis in idem* guarantee must provide for clear and precise rules which allow an individual to predict which acts and omissions are liable to be subject to such a duplication of proceedings and penalties.[26] As demonstrated above and suggested by the Court itself in *BV* and *MR*,[27] the issue of the clarity and preciseness of the rules does, however, already influence the question of whether a legal basis for a limitation of the *ne bis in idem* guarantee can be assumed at all. Conversely, the second and third strict necessity sub-criteria that the Court has identified have independent significance. As second sub-criterion, the ECJ specifically requires that the rules in question ensure coordination between the different authorities, allowing these authorities to offset the disadvantages resulting from the duplication of proceedings.[28] Furthermore, as a third sub-criterion, it is required that the rules oblige the competent authorities to take into account the first penalty already imposed in their assessment of the second penalty. This is to ensure that the severity of all penalties reflects the seriousness of the offences committed.[29] Finally, the Court made it explicit that the rules corresponding to these requirements must also be applied adequately by the competent authorities, meaning that, on the one hand, the two sets of proceedings must have been effectively conducted in a sufficiently coordinated manner and within a proximate timeframe, and, on the other hand, that the overall penalties imposed must adequately correspond to the seriousness of the offences.[30]

IV. Application of Criteria for Limitations of the *ne bis in idem* Principle at the Inter-State Level in the Volkswagen Case

Having clarified the criteria for limitations of the *ne bis in idem* principle including their specifications established by the Court regarding intra-state cases, the question remains to be answered whether these criteria are met in the Volkswagen case (Case C-27/22). Given the transnational dimension of that case, it must be assessed whether the specifications of these criteria developed for intra-state scenarios also allow for an adequate assessment of the legitimacy of limitations of the *ne bis in idem* principle at inter-state level and should thus be applied to the Volkswagen case. These questions will be analysed in the following by discussing the limitation criteria in turn, against the background of Case C-27/22.

1. "Provided for by law"

It has to be noted that a discussion of Case C-27/22 might be cut short. In fact, it seems doubtful whether the very first criterion, stipulating that the limitation of the *ne bis in idem* guarantee must be provided for by law, is met in the present case.

a) Legal basis in EU law

An initial point that needs to be made in this regard is that the legal basis for any limitation of the transnational *ne bis in idem* principle, as enshrined in Art. 50 CFR and Art. 54 CISA, can only be found in EU law. This follows from the very fact that Art. 55 CISA itself defines the cases in which the contracting parties – when ratifying, accepting, or approving the Convention – may declare themselves exempt from being bound by the *ne bis in idem* principle. It clearly contradicts the logic of this provision to accept that Member States could, in principle, at any time and for any case, declare themselves not bound by the *ne bis in idem* guarantee by law. Moreover, any legislation allowing Member States to exempt themselves from being bound by the *ne bis in idem* guarantee whenever they deem it appropriate would affect the essence of that guarantee as such and would, consequently, be incompatible with Art. 52 para. 1 CFR. Accordingly, the Court based the two exceptions to the *ne bis in idem* guarantee that it has recognised so far on provisions of Union law.[31]

b) Legal basis in Case C-27/22?

In the Volkswagen case, the referring court, in its third question, identifies Art. 3 para. 4 and Art. 13 para. 2 lit. e) of

Directive 2005/29/EC on unfair commercial practices[32] as possible legal bases for derogations from the transnational *ne bis in idem* principle.

However, it is not apparent to what extent Art. 3 para. 4 Directive 2005/29/EC could serve as a legal basis for such a derogation. The article stipulates that in case of conflict between the provisions of Directive 2005/29/EC and other Union rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects. So rather than making reference to *ne bis in idem* constellations, this provision aims at resolving conflicts between legal instruments. At best, an *argumentum e contrario* seems possible, stating that Directive 2005/29/EC prevails over every Union rule that does *not* regulate specific aspects of unfair commercial practices. However, this interpretation is extremely broad and not supported by the wording of the provision. In any case, Art. 3 para. 4 Directive 2005/29/EC does not clearly and precisely define the conditions for possible limitations of the *ne bis in idem* principle and does thus definitely not meet the criteria for a limitation of the *ne bis in idem* guarantee to be provided for by law.

A similar conclusion can be drawn for Art. 13 para. 2 lit. e) Directive 2005/29/EC. This provision establishes that Member States, when imposing penalties for infringements of national provisions adopted in application of the Directive, shall take into account *inter alia* the criterion whether penalties have been imposed on the trader for the same infringement in other Member States in cross-border cases. However, this stipulation is limited to situations in which information about such penalties is available through the mechanism established by Regulation (EU) 2017/2394[33]. This latter regulation deals with the cooperation between national authorities responsible for the enforcement of consumer protection laws. It thus specifically refers to administrative proceedings and penalties for unfair commercial practices which can be classified as criminal in the European sense[34] and normally trigger the applicability of the *ne bis in idem* guarantee. Against this background, it seems plausible, on the face of it, to assume that Art. 13 para. 2 lit. e) Directive 2005/29/EC envisages situations principally incompatible with the *ne bis in idem* guarantee and, therewith, implicitly establishes an exception to it.

However, when taking into account the Recitals of Regulation (EU) 2017/2394 and of Directive (EU) 2019/2161[35], introducing Art. 13 para. 2 lit. e) into Directive 2005/29/EC, such an understanding does not seem to have been intended by the European Union legislature. While Recital 29 of Regulation (EU) 2017/2394 explicitly states that the principle of *ne bis in idem* should be respected, Recital 8 of Directive (EU) 2019/2161 even provides that the non-exhaustive and only indicative criteria introduced by Art. 13 para. 2 Directive 2005/29/EC might not be relevant for the imposition of penalties for every infringement. Rather, Member States are explicitly called to also take account of other general principles of law applicable to the imposition of penalties, such as the principle of *non bis in idem*. In light of this, Art. 13 para. 2 lit. e) Directive 2005/29/EC should be understood as only allowing for a duplication of penalties falling outside the scope of application of the *ne bis in idem* guarantee due to their non-criminal nature.

2. Respect for the essence of Art. 50 CFR in Case C-27/22?

Notwithstanding the above, Art. 13 para. 2 lit. e) Directive 2005/29/EC should not be taken as a guarantor for the essence of Art. 50 CFR being duly respected. At the very minimum, it does not clearly and exhaustively define the conditions for a limitation of the *ne bis in idem* guarantee. Quite to the contrary, it forms part of a list of "non-exhaustive" and only "indicative" criteria that shall be taken into account when imposing penalties "where appropriate." Furthermore, Art. 13 para. 2 lit. e) Directive 2005/29/EC does not even specify the intended consequence of taking into account a penalty imposed in another Member State for the same infringement and could, therefore, even be understood as envisaging the Member State engaged in sentencing to completely refrain from imposing a second penalty whenever the *ne bis in idem* guarantee applies.

3. Interim result

It can be concluded that a legal basis for a limitation of the transnational *ne bis in idem* principle is lacking in Case C-27/22. The only provision that on the surface appears to be a candidate for such a legal basis (Art. 13 para. 2 lit. e) Directive 2005/29/EC) definitely does not guarantee that the essence of Art. 50 CFR is respected. It follows that the first criterion for a limitation of the *ne bis in idem* guarantee is not met at all, and compliance with the second criterion is at least not ensured.

4. Considerations on remaining criteria: validity of the ECJ's specifications at transnational level?

In light of the foregoing, the *Volkswagen* Case does not directly call for an analysis of the third, fourth, and fifth criteria for the legitimacy of limitations of the *ne bis in idem* guarantee. Nonetheless, given the utmost importance of the question of justifiability of such limitations at transnational level (in particular if one considers the context of the transnational *ne bis in idem* principle as an enabler of a single area of freedom, security, and justice, generally governed by the principles of mu-

tual recognition and mutual trust),[36] it will be briefly commented on the question of whether the specifications relevant to these remaining criteria developed by the ECJ for intra-state settings should likewise be applied at the inter-state level.

a) The "complementary aims" criterion

Let us recall that, as the third criterion for limitations of the *ne bis in idem* guarantee, it is required that an objective of general interest is pursued in order to justify this limitation and that the ECJ has determined in this regard for intra-state settings that the different proceedings and penalties pursue complementary aims relating to different aspects of the same unlawful conduct for the purpose of achieving this overall objective of general interest.[37] However, at least to date, the Court has not further specified the term "complementary aims," making it very flexible and broad for the time being.[38] In any case, the aim being pursued by proceedings and by a penalty in relation to a specific conduct depends on the legal classification of the conduct in question by the respective Member State. However, given the still rather rudimentary degree of harmonisation of Member States' criminal laws, one and the same conduct will frequently be subsumed under differing provisions in different states. Therefore, it is largely left to chance whether the different national legislations that are applied to a specific conduct pursue the same or complementary objectives.

It follows that the criterion of the pursuit of complementary aims, which makes much sense in a single harmonious national legal system, loses its limiting potential for exceptions from the *ne bis in idem* guarantee when transferred to the still poorly harmonised transnational sphere. Instead, as this criterion is necessarily tied to the legal classification of the respective behaviour in the different Member States, applying it in transnational settings would run directly counter to the factual conception of the notion of "the same offence" in the sense of Art. 50 CFR and Art. 54 CISA, which is independent of the legal classification of the conduct.[39]

b) The coordination requirement and the holistic sentencing approach

Unlike for the "complementary aims" criterion, the specifications developed by the ECJ regarding the strict necessity of limitations of the *ne bis in idem* guarantee seem suitable in a transnational setting as well. In particular, effective and close coordination of the different proceedings should also be required in an inter-state context. Not making such coordination a prerequisite for any limitation of the *ne bis in idem* guarantee would run counter to the very idea of the EU as a single area of freedom, security, and justice. Indeed, every Member State could, provided the other conditions of the respective limitation of the *ne bis in idem* principle are met, simply refuse to cooperate with another Member State and conclude its own proceedings. This would result in a double burden for the suspect, in particular with respect to coercive measures, and could eventually lead to the imposition of penalties not taking into account penalties already imposed in another Member State for the same offence, and thus exceeding what would be proportionate.

Whether coordination has been in place in the Volkswagen case is not apparent from the documents publicly available. At any rate, hypothetically assuming that all the other prerequisites of a limitation of the *ne bis in idem* guarantee were met in this case, the Italian *Consiglio di Stato* would have to take into account the penalty imposed in Germany when determining their fine.

V. Conclusion

The foregoing analysis demonstrated that it seems suitable to apply nearly all specifications established by the ECJ with regard to limitations of the intra-state *ne bis in idem* principle at transnational level as well. The only exception is the requirement of "complementary aims" having to be pursued by the respective proceedings and penalties as it is ill-suited to the still poorly harmonised transnational criminal law setting. However, Case C-27/22, involving the diesel scandal of Volkswagen, fails to even meet the very first criterion for a justification of limitations to the transnational *ne bis in idem* guarantee. There is no clear and precise legal basis for such a limitation and, even if Art. 13 para. 2 lit. e) of Directive 2005/29/EC were to be qualified as such, this provision does not ensure that the very essence of Art. 50 CFR is respected. Thus, the third question referred to the ECJ by the Italian *Consiglio di Stato* will have to be answered in the negative: The provisions laid down in Art. 3 para. 4 and Art. 13 para. 2 lit. e) of Directive EU/2005/29 do not justify a derogation from the *ne bis in idem* principle.

---

1 ECJ, 27 May 2014, Case C-129/14 PPU, *Spasic,* para. 31.
2 ECJ, *Spasic, op. cit.* (n. 1), para. 55.
3 ECJ, 23 March 2023, Case C-365/21, *MR v Generalstaatsanwaltschaft Bamberg.*
4 ECJ, 20 March 2018, Case C-524/15, *Menci,* paras. 44 et seqq.
5 ECJ, 20 March 2018, Case C-537/16, *Garlsson Real Estate,* paras. 46 et seqq.
6 ECJ, 5 May 2022, Case C-570/20, *BV,* para. 31 and paras. 38 et seqq.
7 ECJ, 22 March 2022, Case C-117/20, *bpost,* paras. 49 et seq.
8 In *Nordzucker,* judgment of 22 March 2022, Case C-151/20,

Prof. Dr. Laura Neumann
Professor of Criminal Law and Criminal Procedure Law as well as Economic Criminal Law, University of Bremen

the ECJ departed from its former case law according to which, only in competition law, the *idem* criterion did not only require the same offender and the same facts, but also the same protected legal interest (see ECJ, 7 January 2004, Joined Cases C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P, and C-219/00 P, *Van Aalborg Portland,* and ECJ, 14 February 2012, Case C-17/10, *Toshiba Corporation and Others).* For the first time, the Court only focused on the material acts in competition law as well, as had been the case in all other areas of law since *Van Esbroek* (ECJ, 9 March 2006, Case C-436/04); on this, see M. Cappai and G. Colangelo, "Applying *ne bis in idem* in the aftermath of *bpost and Nordzucker:* the case of EU competition policy in digital markets", *SSRN paper,* posted 1 January 2023, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4344075> (last visited on 21 March 2023), modified version *forthcoming* in Common Market Law Review.

9 Cf. ECJ, *Nordzucker*, *op. cit.* (n. 8), paras. 53 et seqq., making it clear that, in fact, both national authorities had to apply Art. 101 TFEU, i.e., one and the same provision.

10 See summary of the request for a preliminary ruling – Case C-27/22, available at <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=255661&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2595922> (last visited on 21 March 2023).

11 The full name of the Directive is as follows: Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), *O.J.* L 149, 11.6.2005, 22.

12 Whether a penalty is to be classified as criminal in nature is examined by the ECJ, following the so-called *Engel* criteria of the ECtHR (see ECtHR, 8 June 1976, Application nos. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, *Engel et al. v. the Netherlands*, para. 82), on the basis of the legal classification of the infringement in domestic law (which is, however, only the starting point), the nature of the infringement, and the nature and severity of the threatened sanction (see ECJ, 5 June 2012, Case C-489/10, *Bonda,* paras. 36 to 44; ECJ, 7 May 2013, Case C-617/10, *Åkerberg Fransson*, para. 35; ECJ, *Menci, op. cit.* (n. 4), paras. 26 et seqq.; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), paras. 28 et seqq.).

13 Cf. summary of the request for a preliminary ruling – Case C-27/22, para. 16, *op. cit.* (n. 10).

14 Specifically, ECtHR, 27 November 2014, Application No. 7356/10, *Lucky dev v. Sweden*, para. 60; the sequence of procedurally relevant events in *Garlsson Real Estate* was very similar to the one in Case C-27/22 and did, according to the ECJ, not hinder the applicability of Art. 50 CFR (see ECJ, *Garlsson Real Estate, op. cit.* (n. 5), paras. 11 et seqq.).

15 See ECJ judgments in *Menci, op. cit.* (n. 4), para. 40; *Garlsson Real Estate, op. cit.* (n. 5), para. 42; and *bpost, op. cit.* (n. 7), para. 40.

16 ECJ, *BV, op. cit.* (n. 6), para. 31.

17 ECJ, *MR, op. cit.* (n. 3), para. 51.

18 ECJ, *Menci, op. cit.* (n. 4), para. 49.

19 ECJ, *Garlsson Real Estate, op. cit.* (n. 5), para. 51.

20 ECJ judgments in *Menci, op. cit.* (n. 4), para. 49; *Garlsson Real Estate, op. cit.* (n. 5), para. 51; and *bpost, op. cit.* (n. 7), para. 51. In *BV (op. cit.* (n. 6), para. 38), the Court specified that the criterion of a limitation being defined by law is also "satisfied where the individual is in a position to ascertain from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, which acts and omissions will make him or her criminally liable."

21 ECJ, *Menci*, *op. cit.* (n. 4), para. 43; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), para. 45; *BV*, *op. cit.* (n. 6), para. 32.

22 ECJ, *Menci*, *op. cit.* (n. 4), para. 44; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), para. 46.

23 ECJ, *bpost*, *op. cit.* (n. 7), para. 49.

24 ECJ, *Menci*, *op. cit.* (n. 4), para. 46; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), para. 48; ECJ, *bpost*, *op. cit.* (n. 7), para. 48.

25 See the summary of these three criteria for instance in ECJ, *BV*, *op. cit.* (n. 6), para. 36, referring to *Menci*.

26 ECJ, *Menci*, *op. cit.* (n. 4), para. 49; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), para. 51.

27 See again ECJ, *BV*, *op. cit.* (n. 6), para. 31, and ECJ, *MR*, *op. cit.* (n. 3), para. 51.

28 ECJ, *Menci*, *op. cit.* (n. 4), para. 52; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), para. 54; ECJ, *bpost*, *op. cit.* (n. 7), para. 51.

29 ECJ, *Menci*, *op. cit.* (n. 4), para. 55; ECJ, *Garlsson Real Estate*, *op. cit.* (n. 5), para. 56; see ECJ, *bpost*, *op. cit.* (n. 7), para. 51.

30 ECJ, *bpost*, *op. cit.* (n. 7), para. 51.

31 See ECJ, *Spasic*, *op. cit.* (n. 1), para. 57; ECJ, *Nordzucker*, *op. cit.* (n. 8), para. 53.

32 *Op. cit.* (n. 11).

33 Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, *O.J.* L 345, 27.12.2017, 1.

34 However, the Regulation cannot be understood to refer to criminal law *stricto sensu* – cf. for instance Recitals 21 and 29, Art. 2 para. 3, Art. 14 para. 2 lit. a) of Regulation (EU) 2017/2394, *op. cit.* (n. 33).

35 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, *O.J.* L 328, 18.12.2019, 7.

36 See Opinion of Advocate General Spuznar, 20 October 2022, Case C-365/21, para. 55.

37 Again, see ECJ judgments in *Menci*, *op. cit.* (n. 4), para. 44; *Garlsson Real Estate*, *op. cit.* (n. 5), para. 46; and *bpost*, *op. cit.* (n. 7) para. 49; in Case C-27/22, the objective of general interest pursued would be the protection of European consumers (see summary of the request for a preliminary ruling – Case C-27/22, para. 19, *op. cit.* (n. 10)).

38 In *Menci*, for example, the differing degrees of severity of the penalties and the targeting of behaviours with different degrees of social harmfulness seemed to be decisive for the Court to affirm the complementarity of the aims pursued by the administrative penalties, on the one hand, and the criminal penalties, on the other hand (see ECJ, *Menci*, *op. cit.* (n. 4), para. 45). Generally, it would also be conceivable to make reference to the respective legal interests protected.

39 Standing case law since ECJ, *Van Esbroek*, *op. cit.* (n. 8), para. 42.

Non-Conviction Based Forfeiture in Canada: The Example of Three Outlaw Motorcycle Gang Clubhouses

Jeffrey Simser

A 2023 non-conviction based (NCB) forfeiture order was recently issued against three clubhouses in Canada. Each served as the chapter headquarters for an outlaw motorcycle gang. Clubhouses form the base of operations for their organized criminal activities. The protracted litigation started in 2007, and a Canadian appellate court found in February 2023 that the clubhouses were forfeitable as instruments, as they supported the organized criminal activities of outlaw motorcycle gangs. The court overturned a trial ruling that part of the NCB law was unconstitutional. The court also held that each clubhouse served as a "safe house" for the respective gang, namely as a place where business could be conducted away from the prying eyes of the police. The clubhouses were also intelligence hubs, where members could discuss their criminal business, their rivals, and the techniques used by police to interdict them. Lastly, the court found that each club-house operated as a "planted flag" marking the territorial jurisdiction of the outlaw motorcycle gang, announcing to both customers and rivals that this was its territory. This ruling will have an important impact on organized crime cases mov-ing forward, giving law enforcement an NCB option to apply. This article summarizes the cases and examines the type of evidence used in court to tackle organized crime. It concludes with the analysis of a similar case in New Zealand.

I. How Does Non-Conviction Based Forfeiture Work in Canada?

Non-conviction based (NCB) forfeiture, called civil forfeiture in Canada, is a remedial statutory device designed to recover the proceeds and instruments (property used to facilitate crime) of unlawful activity. Canada first adopted NCB forfeiture in 2001, and there are now nine jurisdictions in Canada that have such laws: the constitutional division of powers assigns civil law authority to subnational jurisdictions. Canada adopted the American *in rem* approach, meaning that proceedings are brought before civil court against the object of forfeiture, not against the person associated with the property. As a result, Canadian court cases may have unusual names like *Ontario (Attorney General) v. $232,405 in Canadian Currency*.[1] NCB cases operate independently of criminal law cases, which are brought against individuals; the criminal law matches a prohibition with an appropriate penalty to enable a criminal charge to be brought against an individual. Canada has conviction-based forfeiture provisions in its criminal law.

In 2009, Canada's highest court ruled that the Canadian NCB laws were constitutional, finding their dominant purpose a civil one: making crime unprofitable by capturing the fruits of crime and making resources unavailable to fund future crime.[2] This ruling addressed a proceeds case. In an NCB case, property with an unlawful provenance is a proceed. Illicit narcotics are exchanged for cash on the street, and that cash is a proceed. NCB cases are brought before a civil court, where the judge is asked to inquire into the title. If the title was generated through crime, the court is empowered by statute to extinguish that title. In the common law world, property law despises a void. NCB law prevents a void by allowing the court to forfeit the property to the state, where it can be made available for, amongst other things, victim compensation. Instruments can also be forfeited, although the court has a slightly different ground for their forfeiture. An instrument is a piece of property that makes the labour of crime possible. The court must examine the use of the property: if this property is not forfeited, will it be used again? As a safeguard, NCB statutes confer on the court a jurisdiction to refuse to issue an order that would clearly not be in the interest of justice. If the state makes out all technical elements required for a case, the court can still refuse or limit forfeiture if the outcome would be manifestly harsh or inequitable. For example, a very valuable property could be implicated in a minor crime and the court could refuse to issue an NCB forfeiture order.[3] In a recent outlaw motorcycle gang case, the appellate court in British Columbia examined the constitutionality of Canada's NCB instrument provisions.[4]

II. Outlaw Motorcycle Gangs and Organized Crime

In 2007, a case was brought against a clubhouse in Nanaimo, British Columbia, which belonged to the Hells Angels' Motorcycle Club (HAMC), a notorious outlaw motorcycle gang. Two other HAMC clubhouses, in Vancouver and Kelowna, were later added to the proceedings. In British Columbia, NCB cases are initiated by the director of civil forfeiture (hereinafter: "the Director"). At trial in the above-mentioned case, the director adduced evidence about the HAMC. At the time of trial, there were 463 HAMC chapters

with roughly 6000 members in 56 countries. Canada has 34 active chapters. HAMC chapters must comply with international membership rules (as well as Canadian and local rules), pay dues, participate in "motorcycle runs," and organize shifts to ensure that the clubhouse buildings are always occupied. Chapters have weekly member-only meetings and have relative independence within the broader HAMC world. Promotion to "full member" must be approved by all members of the chapter. Undesirables, including "snitches, junkies, cops or ex-cops" are prohibited. Anyone who has joined or chosen to work with any law enforcement agency is ineligible for membership. At regional, national, and international meetings, members discuss organized crime proceedings and the activities of rival outlaw motorcycle gang clubs. Members also exchange information about the existence and investigation of potential "snitches" and contribute to defence funds for members facing criminal charges.[5]

Those who have a passing familiarity with organized crime might find the HAMC operating model strange. Organized criminals aspire to blend in, driving modest vehicles (so as not to attract "heat" from law enforcement) and presenting as respectable members of their community. Outlaw motorcycle gangs run on the "power of the patch" and use their well-known propensity for violence to intimidate and control local criminal markets. Clubs have a "no burn" rule for drug transactions, meaning that if they agree to sell you narcotics, they will honour the transaction. Outlaw motorcycle gangs want a reputation of reliability. Reliability builds sales volume, giving the organization the wherewithal to source wholesale narcotics offshore. Locally, the HAMC controls the market within its territory. Violence ensures that non-affiliated drug dealers will either pay a tax or source their drugs with the local chapter. The HAMC members wear a "death head" patch on the back of their jackets; only members are allowed to wield that patch, which represents and projects the power of the club.[6] There is one other marked physical declaration: the presence of an outlaw motorcycle gang clubhouse.[7]

Clubhouses are central to the outlaw motorcycle gang business model. The three clubhouses in the aforementioned Canadian NCB case were two-story fortified buildings on fenced and gated property. The fences ensure privacy: people on the street, including police, cannot see what is going on in the compound. The front doors are made of metal and open outwards; they are designed to prevent forced entry. Where there are windows, they are made of bulletproof glass. Cameras and a security system monitor the property. Inside the club, a member-only section for secret meetings is set off from the main entertainment area. The buildings include kitchens, bars, recreational areas, storage areas, bedrooms, and a gym.

The evidence adduced in court showed that these clubhouses served three operational objectives for the outlaw motorcycle gang. First, they operate as safe houses. This allows members to plan crimes, including drug trafficking. Clubhouses allow for weapons storage. Members can collectively muster at the clubhouse to travel and commit crime. Disputes within the gang can be resolved privately in the clubhouse. Second, the clubhouses are intelligence hubs. Members can network and develop criminal enterprise opportunities. Donations are solicited to fund criminal defences for members facing prosecution. Information can be stored and disseminated about fellow members, rivals, "snitches," and undercover police officers. Police methods and criminal countermeasure strategies can be safely discussed in the clubhouse. Third, the clubhouse represents a "planted flag" that marks the outlaw motorcycle gang's territory. The building serves as a reminder (and warning) to rivals that this is HAMC turf.

III. Extended NCB Litigation

The litigation in this case was extensive and long. In 2007, a freezing order (called an interim preservation order by the statute) was obtained for the first clubhouse. Over time, some assets were released (e.g. motorcycles) and others were added (two more clubhouses). The pre-trial proceedings were described by the assigned trial judge as a "procedural quagmire," and most steps were heavily contested. Throughout a protracted pre-trial process, the lawyers for the outlaw motorcycle gang challenged the director's evidence and use of experts as well contesting numerous points of law. Finally, after eleven years of litigation, the matter went to trial. Two years later, in 2020, the trial judge issued a massive 327-page judgment and ordered the clubhouses returned to the outlaw motorcycle gang. The principal gravamen for the trial judge was that NCB forfeiture for instruments was an impermissibly ersatz form of criminal law. According to the trial judge, the statute called on the Director to prove the propensity to commit crimes. The trial judge found that the effect of the NCB instruments provision was to suppress, criminalize, and punish offenders, a matter reserved for criminal law and criminal standards of proof (beyond a reasonable doubt, in Canada, as opposed to the civil standard of balance of probabilities). The trial judge's findings on evidence and the constitutionality of the instrument's provisions was firmly overturned in 2023 by the Court of Appeal. That court ruled that the purpose of NCB forfeiture for an instrument was to disable the property and deter future unlawful activities by removing it from a criminal. The Court of Appeal found that this was a constitutionally valid exercise of the civil law.

The Court of Appeal also overturned the evidentiary findings of the trial judge, criticizing his refusal to admit certain evidence and his application of an improperly elevated standard of proof. The court drew attention to several facts: The clubhouses were a safe space in which outlaw motorcycles gangs could plan future crimes, often using erasable whiteboards to discuss activities silently, without the risk of being overheard or detected by police. Members of the gang could share criminal disclosure packages to understand how the police operate and then develop strategies to evade future detection. The clubhouses stored information on agents and informants, again with a view towards evading future investigations. The buildings were outfitted with measures to prevent surveillance or monitoring by police; the clubs had a penchant for secrecy and a preoccupation with "rats and snitches;" many members of the club had been implicated in past crimes and had engaged others to commit crimes and acts of violence. Finally, the clubhouses reinforced the presence of the outlaw motorcycle gang in the territory, a presence backed up by propensity to engage in violence against anyone who dared to cross it. Against this factual background, the Court of Appeal issued orders of forfeiture against the three clubhouses.

IV. What's Next?

This case, launched in 2007, was one of the first British Columbia civil forfeiture cases to tackle organized crime. Every step of the case was fiercely contested. The voluminous 2020 decision of the trial judge was worrying on numerous fronts. Had that decision stood, the use of NCB forfeiture in Canada for organized crime cases would have been curtailed. The trial judge rejected expert evidence from an experienced organized crime investigator and then found there was insufficient evidence to support forfeiture. In its 2023 decision, the Court of Appeal overturned these findings and clarified the law. The outlaw motorcycle club has sought leave to appeal this decision to the Supreme Court of Canada.[8] Of related interest, the Supreme Court of Canada ruled in 2009 that civil forfeiture was constitutional, but that case involved proceeds not instruments.[9]

Those interested in outlaw motorcycle gang clubhouses and NCB forfeiture might also wish to read a New Zealand decision: *Commissioner of Police v. Richardson*.[10] In this decision, an outlaw motorcycle gang called the "Head Hunters" faced an NCB forfeiture proceeding in respect of its clubhouse near Christchurch. In New Zealand, NCB proceedings are brought by the police, who in this instance tendered evidence that the Head Hunters had engaged in illegal gaming and in the sale of methamphetamine. Not only did the gang sell drugs, but, like their Canadian counterparts, it also "taxed" other drug dealers who operated in its territory. Unlike the Canadian litigation, however, the police were able to adduce sufficient evidence for the court, tracing the proceeds of crime to renovations of the clubhouse; these findings supported a right of NCB forfeiture of the clubhouse as a proceed. For law enforcement, a "proceeds" theory, as used in New Zealand, appears to be a less complicated pathway to an NCB forfeiture based on an instruments theory.

Jeffrey Simser
Barrister and Solicitor in Toronto, Canada

1 2022 ONSC 7353.
2 *Chatterjee v. Ontario (Attorney General)*, 2009 SCC 19.
3 J. Simser, *Civil Asset Forfeiture in Canada* (Canada Law Book 2011 – present, loose-leaf, updated twice annually).
4 *British Columbia (Director of Civil Forfeiture) v. Angel Acres Recreation and Festival Property Ltd., 2023 BCCA 70.*
5 *British Columbia (Director of Civil Forfeiture) v. Angel Acres Recreation and Festival Property Ltd.,2020 BCSC 880.*
6 See, for example, P. Edwards and L. Najera, *The Wolfpack* (Toronto: Penguin, 2022); J. Sher and W. Marsden, *The Road to Hell* (Toronto: Penguin, 2004).
7 In *R. v. Lindsay*, 2009 ONCA 532, the court found that the HAMC relied on its "patch" and reputation for violence to collect debts as part of an extortion scheme; the court ruled that the HAMC was a criminal organization.
8 Angel Acres Recreation and Festival Property Ltd. and All Others Interested in the Property, et al. v. Director of Civil Forfeiture, et al. Leave sought April 17, 2023, file #40688.
9 *Chatterjee v. Ontario (Attorney General)*, 2009 SCC 19.
10 2022 NZHC 3184.

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
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; Dr. 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: Katharina John, 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: Ines Hofmann, Max Planck Institute for the Study of Crime, Security and Law, Freiburg
Printed by: Stückle Druck und Verlag, Ettenheim, Germany

The publication is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF)

Co-funded by the European Union

ISSN: 1862-6947

Practical Information

Articles in eucrim are subject to an editorial review. The journal 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.

More information at our website: https://eucrim.eu

Contact

Thomas Wahl
Max Planck Institute for the Study of Crime, Security and Law
Guenterstalstrasse 73
79100 Freiburg i.Br., Germany
Tel: +49(0)761-7081-256 or +49(0)761-7081-0 (central unit)
E-mail: info@eucrim.eu

https://eucrim.eu/

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