Vol. 92 issue 2, 2021

RIDP

Gert Vermeulen,
Wannes Bellaert *(Eds.)*

EU Criminal Policy: Advances and Challenges

Revue Internationale de Droit Pénal
International Review of Penal Law
Revista internacional de Derecho Penal
Международное обозрение уголовного права
刑事法律国际评论
المجلة الدولية للقانون الجنائي
Revista Internacional de Direito Penal
Rivista internazionale di diritto penale
Internationale Revue für Strafrecht

IRCP

MAKLU

AIDP – Association Internationale de Droit Pénal | The International Association of Penal Law is the oldest association of specialists in penal law in the world. Since 1924, it is dedicated to the scientific study of criminal law and covers: (1) criminal policy and codification of penal law, (2) comparative criminal law, (3) international criminal law (incl. specialization in international criminal justice) and (4) human rights in the administration of criminal justice. The Association's website provides further information (http://www.penal.org).

RIDP – Revue Internationale de Droit Pénal | The International Review of Penal Law is the primary publication medium and core scientific output of the Association. It seeks to contribute to the development of ideas, knowledge, and practices in the field of penal sciences. Combining international and comparative perspectives, the RIDP covers criminal law theory and philosophy, general principles of criminal law, special criminal law, criminal procedure, and international criminal law. The RIDP is published twice a year. Typically, issues are linked to the Association's core scientific activities, i.e. the AIDP conferences, Young Penalist conferences, world conferences or, every five years, the International Congress of Penal Law. Occasionally, issues will be dedicated to a single, topical scientific theme, validated by the Scientific Committee of the Association, comprising high-quality papers which have been either presented and discussed in small-scale expert colloquia or selected following an open call for papers. The RIDP is published in English only.

Peer review: All contributions are subject to double-layered peer review. The primary scientific and peer review responsibility for all issues lies with the designated Scientific Editor(s). The additional scientific quality control is carried out by the Executive Committee of the Editorial Board, which may turn to the Committee of Reviewers for supplementary peer review.

ISSN – 0223-5404
ISBN 978-90-466-1134-0
D/2022/1997/1
NUR 824
BISAC LAW026000
Theme: LNF, LAR

Maklu- Publishers
Somersstraat 13/15, 2018 Antwerpen, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com, www.isbs.com

Editorial Board

Summary

EU CRIMINAL JUSTICE AND LAW ENFORCEMENT COOPERATION: NEVER A DULL MOMENT

By Gert Vermeulen[*]

Initially, ie until the end of the 1990s, in the context of the European Political Cooperation and under the Maastricht Treaty, EU integration in the area of criminal law centred primarily around the regional deepening of traditional judicial cooperation in criminal matters (especially in the areas of extradition and MLA) and the development of law enforcement cooperation (including by the setting up of Europol in 1995 and the provision of enhanced customs cooperation, supported by a Customs Information System (CIS)). The Amsterdam Treaty (as from May 1999) radically broadened its scope by formally allowing for (albeit limited) harmonisation in the area of substantive criminal law, as did the Lisbon Treaty (as from December 2009) in the area of procedural criminal law. Both judicial and law enforcement cooperation were boosted over the years with the introduction of the mutual recognition principle (ie the cornerstone for judicial cooperation between the EU Member States, since October 1999) and of the principle of availability (ie the lead principle for horizontal law enforcement cooperation between the Member States since November 2004), and with the setting up (and further development) of Eurojust, the establishment of a European Public Prosecutor's Office (EPPO) (for crime affecting the EU budget) and the further development of Europol.

Undeniably, after three decennia, the EU criminal law corpus is impressive – a core component of the EU's 'Area of Freedom, Security and Justice', building on and adding to (both real and presumed) trust between the Member States.

Notwithstanding, since 2020, the *von der Leyen* Commission has been quite unstoppable in its ambition, launching a tsunami of legislative proposals, including in the sphere of EU criminal law, largely framed in its new EU Security Union Strategy (2020-2025).[1] The latter centres around four axes: (i) achieving a future proof security environment (by enhancing cybersecurity and protecting critical infrastructures and public spaces), (ii) tackling evolving threats (such as cybercrime and illegal content online), including by boosting law enforcement's digital capacity (via AI, big data and high performance computing tools), (iii) protecting Europeans from terrorism and organised crime, and (iv) building a strong European security ecosystem, *inter alia* by strengthening Europol.

---

[*] Senior Full Professor of European and international Criminal Law and Data Protection Law, Director of the Institute for International Research on Criminal Policy (IRCP), of the Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES) and of the Smart Solutions for Secure Societies (i4S) business development center, all at Ghent University; General Director Publications of the AIDP; Editor-in-Chief of the RIDP. For correspondence: <gert.vermeulen@ugent.be>.

[1] European Commission, 'Communication from the Commission on the EU Security Union Strategy' COM(2020) 605 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605> accessed 17 May 2022.

This special issue on 'EU criminal policy. Advances and challenges' discusses and assesses some of these new developments, building on selected papers from a publication project[2] with international research master graduates in EU criminal policy at Ghent University.

The first two papers centre around Europol. After its Convention-based inception in 1995, Europol was further developed and upgraded by several Protocols, a 2009 Decision and a 2016 Regulation. In December 2020, the *von der Leyen* Commission, as part of its Security Union Strategy, proposed yet a newer Europol Regulation, to further strengthen the Agency. The text was agreed in May 2022[3] by the EU co-legislators (ie the Council and the European Parliament) and introduces broader/enhanced competences for Europol in a range of areas: research and innovation (aimed at helping member states in their use of emerging technologies, exploring new approaches and developing common technological, including AI-based, solutions), cooperation with third countries (more autonomy), cooperation with EPPO (by offering it essential analysis support), Schengen Information System (SIS) alerts (by granting it an active (support) role in entering and proposing SIS alerts on the basis of data transmitted by third countries or international organisations, including on foreign fighters), own-initiative investigations (also into non-cross-border crimes affecting a common interest covered by a Union policy), processing of large and complex (big) data sets, and cooperation with private parties. The latter two developments are addressed in this issue.

Dante Hoek and *Jill Stigter* (Europol: An Overwhelming Stream of Big Data) discuss the big data development at Europol level, for which the 2022 Regulation provides an ex-post legitimation and legal basis. After the 2015 Paris (and 2016 Brussels) terrorist attacks, the French authorities had provided Europol with 16,7 Terabytes of data, including on persons falling outside of the scope of Europol's mandate. Notwithstanding, in the context of taskforce *Fraternité,* Europol started processing the data in order to find linkages to persons formerly unrelated to crime, for which it was admonished by the European Data Protection Supervisor (EDPS) in 2020. In response, the European Commission proposed to amend the Europol Regulation in this respect, by allowing Europol the necessary scope and time for pre-analysis of received large data files, ahead of data subject categorisation in line with its traditional mandate. On the eve of an ultimate agreement between the co-legislators on the new Regulation, the EDPS ordered Europol to delete its incompatible data, which luckily will be avoided by a transitional regime agreed in the new Regulation.

---

[2] Facilitated by Wannes Bellaert, PhD Researcher and Academic Assistant, Institute for International Research on Criminal Policy (IRCP), Ghent University. His role in selecting, upgrading and updating the submitted papers has been invaluable, even co-authoring two of them. For correspondence: <wannes.bellaert@ugent.be>.

[3] Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, PE-CONS 8/22, 11 May 2022, <https://data.consilium.europa.eu/doc/document/PE-8-2022-INIT/en/pdf> accessed 17 May 2022.

Wanqi Lai and *Amalia Van Vaerenbergh* (Europol and its Growing Alliance with Private Parties) discuss Europol's enhanced role in working directly with private parties. Especially when it concerns cybercrime, online terrorist or extreme content, and online child sexual abuse material, relations with private parties, especially internet and communication service providers, have become key for law enforcement. Until now, Europol was generally not allowed to have direct contacts with private parties, except through the EU Internet Referral Unit (IRU), established in 2015 and part of Europol's European Counter Terrorism Centre, *inter alia* for notice and take-down procedures. The 2022 Regulation positions Europol as an EU hub to receive multi-jurisdictional data sets directly from private parties, which the Agency may pre-process in view of dispatching towards the relevant EU member state jurisdiction(s). In specific instances, ie in order to prevent the dissemination of terrorist or violent extremist content or child sexual abuse material, Europol is granted wider possibilities in directly working with private parties. The paper discusses both the new regular and wider competences.

A third paper relates to the harmonisation (or approximation) of substantive criminal law. As stated above, the EU's competence in this respect is limited. Unless approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to (non-criminal law) harmonisation measures (such as the environment, or entry, transit and residence), approximation of the Member States criminal law is limited to certain areas of crime only, ie 'particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis'. The areas of crime – the so called Eurocrimes (an initial list of was already provided in Article 29 of the post-Amsterdam TEU) – are exhaustively listed in Article 83.1 TFEU: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. In principle, the list is extendable, only after unanimous acceptance by the Council of the EU. The 2020 announcement by the *von der Leyen* Commission of its intention to extend the Eurocrimes list with hate speech and hate crime (which it has effectively proposed in December 2021)[4] has sparked a lot of discussion. The primary reason therefore is the explicit incorporation of LGBTIQ hate, by including sexual orientation, gender identity, gender expression and sex characteristics as protected grounds. Though in line with the Commission's LGBTIQ Equality Strategy 2020-2025, certain (Eastern European) member states are not keen – to state the least – to accepting a mandatory criminalisation of LGBTIQ hate speech and hate crime.

[4] European Commission, 'A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime' COM(2021) 777 final, 9 December 2021 <https://ec.europa.eu/info/sites/default/files/1_1_178542_comm_eu_crimes_en.pdf> accessed 31 May 2022.

Alice Ballotta and *Eline Danneels* (Criminalising LGBTIQ Hate Speech and Hate Crime: Stress Test for the EU's Approximation Powers) explore and analyse various legal options to criminalise (LGBTIQ) hate speech and hate crime at EU level, both based on and beyond the option of building on Article 83.1 TFEU and extending the Eurocrimes list.

A fourth paper deals with a core component of the 2020-2025 EU Security Union Strategy, ie the proposed new Cybersecurity Directive, on which the co-legislators have reached political agreement just in May 2022.[5] Whilst traditional criminal law attention logically focuses on cybercrime, it bears relevance to broaden the perspective to cybersecurity. Whilst cybercrime remains very high on the EU agenda, related substantive criminal law harmonisation (with an initial framework decision on attacks against information systems of 2005, replaced by the 2013 Cybercrime Directive) and cooperation in criminal matters (supported by the European Cybercrime Centre (EC3), established within Europol in 2013) have already been stepped up in quite early a phase of EU integration in criminal matters. In addition, all 27 Member States (except Ireland) have also ratified the Council of Europe's Budapest Convention on Cybercrime (ETS No. 185). Moreover, the EU is well underway to establish its own tools for direct cooperation with (foreign) providers in collecting e-evidence in criminal matters. Legislative action in the broader sphere of cybersecurity is much more recent and developing fast. The first EU-wide legislation on cybersecurity in the EU is as young as 2016, when the Directive on Security of Network and Information Systems (the NIS Directive) introduced a network of Computer Security Incidents Response Teams (CSIRTs) in the Member States. In 2019, with the Cybersecurity Act, the EU Agency for Cybersecurity (ENISA), which had organically developed and was ad hoc prolonged on several instances, was given a permanent mandate, more resources and new tasks. It must maintain the newly developed European cybersecurity certification framework (for products and services) and is mandated to offer operational assistance in Member State level cybersecurity incidents and to support the coordination of the EU in case of large-scale cross-border cyberattacks, in collaboration with EC3. The Member States CSIRTs have a counterpart at the level of the EU institutions, bodies and agencies, ie the EU Computer Emergency Response Team (CERT-EU). The *von der Leyen* Commission, as part of the new EU Cybersecurity Strategy 'for the Digital Decade',[6] which it launched together with *Josep Borrell*, the EU's High Representative for Foreign Affairs and Security Policy, has proposed yet another centralised body, ie the so called Joint Cyber Unit (JCU). It will be a new platform (clearly with su-

[5] Council of the EU, 'Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament', 13 May 2022 <https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Strengthening+EU-wide+cybersecurity+and+resilience+%u2013+provisional+agreement+by+the+Council+and+the+European+Parliament> accessed 31 May 2022.

[6] European Commission, 'Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade' JOIN(2020) 18 final, 16 December 2020 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN> accessed 31 May 2022.

pranational ambition), constructed close to ENISA and CERT-EU, aimed at strengthening 'civilian, *law-enforcement* [emphasis added], diplomatic and cyber defence communities' at EU and Member State levels 'to prevent, deter and respond to cyberattacks'.

Fatima El Kaddouri and *Jasper De Vooght* (The New Cybersecurity Directive: Making the EU the Safest Place Against Cyberattacks?) focus on the newest legislative development, ie the proposed Cybersecurity Directive, also called the NIS 2 Directive. The proposal, being also part of the EU Security Union Strategy, was tabled by the *von der Leyen* Commission in December 2020, together with the aforementioned new EU Cybersecurity Strategy. The paper addresses the reasons for revision of the initial NIS Directive, explores alternative policy options, and critically assesses whether the flaws surrounding the initial NIS Directive (a troublesome transposition and fragmentated implementation, resulting *inter alia* in a low level of cyber resilience) have now been sufficiently tackled. Even if meanwhile the co-legislators have reached political agreement on a final version of the text in May 2022, many of the critiques remain equally valid.

A fifth paper ties in with mutual trust issues. These affect the mutual recognition principle that underlies the EU's instruments on judicial cooperation in criminal matters since the Tampere Summit in 1999, including the European Arrest Warrant (EAW). Since 2016 (in *Aranyosi & Căldăraru v Generalstaatsanwaltschaft Bremen*, confirmed *inter alia* in 2018 in *ML* and in 2019 in *Dorabantu*), the Court of Justice of the European Union (CJEU) has accepted/warranted the non-execution of an EAW in case the person sought runs the risk of being subjected to systemic substandard prison conditions (in violation of the right not to be subjected to inhumane or degrading treatment) in the Member State having issued the EAW. In doing so, the Court has formally rebutted the presumption that EU Member States can be trusted to fully comply with human rights, which was underlying the mutual recognition principle since its introduction in 1999. As from 2018 (in *Minister for Justice and Equality*, relating to concerns about the independency of the judiciary affecting the right to a fair trial, and in 2020 in *Openbaar Ministerie (Indépendance de l'autorité judiciaire d'émission))*, the CJEU broadened its position, in that Member States' presumed compliance with fundamental rights may/must also be doubted if the rights position of the person concerned is likely to be affected by systemic rule of law issues (as *in casu* in Hungary and Poland) in the Member State issuing an EAW.

Ellen Verschuere and *Véronique Charyton* (Safeguarding Mutual Recognition by Safeguarding the Rule of Law?) engage with the EU's growing alertness and assertiveness about rule of law challenges in the Member States. Since the CJEU in 2018 in *Associação Sindical dos Juízes Portugueses* confirmed that it may express itself about the rule of law situation in a Member State, not only national judges (in EAW procedures, *supra*) have initiated CJEU preliminary rulings. Also the European Commission has launched infringement procedures before the Court where it assumed certain internal Member State reforms to be contrary to the (EU) rule of law. A gamechanger may be the so called Conditionality Regulation (in full: Regulation on a general regime of conditionality for the protection of the Union budget), adopted by the co-legislators in December 2020. The Regulation allows for a suspension of the payment of EU funds (including from the 800 billion Next

Generation EU post-covid economic recovery fund) to Member States when linked to a breach of the rule of law, eg for lack of proper domestic investigation into fraud against the EU budget/with EU funds or of cooperation with EPPO. The paper analyses to which extent the Conditionality Regulation may realistically be used to remedy rule of law problems and thereby possibly overcome EAW discussions.

The last paper deals with the issue of terrorist content online, which the EU has now decided to also regulate in complementing its historically well-developed counter terrorism criminal policy. In the European Political Cooperation phase, preceding the EU, initial intergovernmental police and judicial cooperation between the Member States of the then European Communities (EC) centred wholly around terrorism. The issue triggered the setting up in the mid-1970s of the Trevi (*terrorisme, radicalisme, extrémisme, violence internationa*le) police cooperation group, which later in time conceptualised a future Europol and established its forerunner in June 1993, ie even before the entry into force of the Maastricht (EU) Treaty. Logically, terrorism features amongst Europol's key mandated crime areas since its very conception. The same goes for Eurojust. Dissatisfaction with the 1977 CoE Convention for the Suppression of Terrorism (which still allowed a political offence for terrorism in extradition law) was also underlying the 1977 call by then French President *Giscard d'Estaing* for an intergovernmental *Espace judiciaire européen* between the EC Member States. In 1996, ie in the early EU phase, the Member States effectively ruled out the political offence exception for terrorism. After 9/11, using its brand new substantive criminal law harmonisation powers under the Amsterdam Treaty, the EU adopted, in June 2002, its first binding minimum standards for the criminalisation and punishment of terrorism (the definition was expanded over the years, currently reflected in Directive (EU) 2017/541). Further, the EU (as other international forums) broadened its anti-money laundering policy to countering the financing of terrorism. It even allows a Europol-enabled transfer of SWIFT intra-European interbank financial transaction information to the US Treasury (and CIA) under the Terrorist Financing Tracking Programme (TFTP). The fight against foreign jihadi terrorist and homegrown fighters is since many years central to the case and analysis work of Eurojust and Europol, where the EU decided to establish an operational European Counter Terrorism Centre (ECTC). Over time, the EU has also taken several initiatives to tackle terrorist content. Reference was already made above to the ECTC/Europol-based EU IRU, which, in addition to producing strategic insights into and steering information on jihadist terrorism, facilitates and initiates notice and take-down procedures for malicious terrorist content online.

Wannes Bellaert, Visara Selimi and *Robin Gouwy* (The End of Terrorist Content Online?) critically assess the EU's newest legislation on the matter, adopted mid-2021: the Terrorist Content Online Regulation.[7] It grants the Member States' competent authorities the power to issue removal orders to service providers offering services in the EU, requiring

[7] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), *OJ* L 172, 31 May 2021, 79–109.

them to remove terrorist content or disable access to it in all Member States. While its objective may be justified, its impact on the right to free speech is undeniable.

Whilst the current issue focuses on a selection of key EU criminal policy developments initiated in 2020, mostly linked to the new EU Security Union Strategy, the *von der Leyen* Commission has not exactly been sitting on its hands since.

To start with, it has proposed further substantive criminal law approximation in two mandated areas. On the basis of Article 83.2 TFEU, it has proposed, in December 2021, to enhance criminal law protection of the environment by revising the Environmental Crimes Directive.[8] In March 2022, building on the Eurocrimes list of Article 83.1 TFEU, it has proposed to step up the combating of domestic violence and violence against women.[9] In doing so, the Commission wants to make sure the goals of the CoE 2014 Istanbul Convention on preventing and combating violence against women and domestic violence (which not all Member States have ratified or implemented sufficiently) are effectively achieved within the remit of the EU. The proposal targets *inter alia* the mandatory criminalisation of rape based on lack of consent (currently, the use of force or threat remains a constituent element for rape in certain Member States) and female genital mutilation. Going beyond the Istanbul Convention, certain forms of cyber (sexual) violence will equally have to be criminalised throughout the EU.

In July 2021, the *von der Leyen* Commission has proposed its new anti-money laundering (AML) and countering of the financing of terrorism (CFT) legislative package, encompassing two regulations and a directive, and entailing a proposal to establish a new Anti-Money Laundering Authority (AMLA).[10] The proposals aim at further strengthening of

[8] European Commission, 'Proposal for a Directive on the protection of the environment through criminal law and replacing Directive 2008/99/EC' COM(2021) 851 final <https://ec.europa.eu/info/sites/default/files/1_1_179760_prop_dir_env_en.pdf> accessed 17 May 2021.

[9] European Commission, 'Proposal for a Directive on combatting violence against women and domestic violence, COM(2022) 105 final, 8 March 2022 <https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/com_2022_105_1_en.pdf#:~:text=The%20current%20proposal%20aims%20to%20effectively%20combat%20violence,to%20justice%3B%20victim%20support%3B%20prevention%3B%20coordination%20and%20cooperation> accessed 17 May 2022.

[10] European Commission, 'Proposal for a Regulation establishing the Authority for Anti-Money Laundering and Countering Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010', COM(2021) 421 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421> accessed 17 May 2022; European Commission, 'Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering of terrorist financing' COM(2021) 420 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420> accessed 17 May 2022; European Commission, 'Proposal for a Regulation on information accompanying transfers of funds and certain crypto-assets (recast)' COM(2021) 422 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422> accessed 17 May 2022; European Commission, 'Proposal for a Directive on the mechanism to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849' COM(2021)423 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423> accessed 17 May 2022.

the EU's already impressive preventative and repressive arsenal (both legislative and institutionally) to tackle money laundering and terrorism financing (far-reaching reporting obligations, criminal law approximation, an EU-wide network of Financial Intelligence Units (FIUs) with a dedicated secure communication infrastructure (FIU-net) and ample information access and exchange capabilities with the Member States' central bank registries and law enforcement authorities at EU and Member State levels, fully mandated agencies like Europol, Europol and EPPO, etc). AMLA will be established to support, instruct and coordinate FIU action in and between the Member States, to host FIU-net and to conduct joint (data-driven) analysis, even if Europol is already conducting full-scale crime analysis on AML/CFT and is running the European Financial and Economic Crime Centre (EFECC). Moreover, AMLA will be granted the capability of referring cases directly to the Member States' competent authorities in criminal matters, notwithstanding that Europol and Eurojust already have a right of initiative to ask the competent authorities to initiate investigations/prosecutions into AML/CFT and that EPPO has been mandated to exercise those functions directly in the Member States for money laundering relating to crimes affecting the EU budget. Whilst the Commission's proposal entails that AMLA will have to conclude strategic working arrangements with Europol, Eurojust, OLAF (the European Anti-Fraud Office) and EPPO, it is hard to see how the establishment of yet another body (and the ensuing additional complexity and layers) will make things better for the competent authorities on the floor, ie in the Member States. Admittedly, this is probably not even the Commission's goal. It essentially distrusts horizontal cooperation between the Member States, exemplified by the proposed granting of a genuine supervisory role to AMLA over the national FIUs, entailing even a direct supranational exercise of risk assessment for the most risky enterprises in the EU.

The Commission's belief in and hunger for agentification and supranationalisation is, honestly, worrisome. In addition to AMLA, the aforementioned JCU (Joint Cyber Unit) and of course the EPPO, it has proposed yet two other centralised bodies, ie a new Centre on Child Sexual Abuse Material (CSAM) and a Customs Agency, all with (supranational) ambitions into the sphere of criminal justice and law enforcement.

The new EU Centre on CSAM, proposed in May 2022, is aimed to function as a clearing house and comprehensive reporting centre, clearly modelled after NCMEC (the US' National Centre for Missing and Exploited Children). According to the proposed Regulation,[11] service and communication providers (including of number-independent OTT messenger services like WhatsApp, FB Messenger, WeChat, Viber etc) will have to report alleged CSAM based on mandatory screening of images against existing databases and AI-based pattern recognition. Surely, parallels can be drawn with the Terrorist Content Online Regulation (*supra*), even if the CSAM Regulation may well will put data protection and the confidentiality of (electronic) communications even more at risk. The new Centre – it hardly surprises – will also have to filter information towards the competent

[11] European Commission, 'Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final <https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 17 May 2022.

law enforcement authorities in the Member States, and of course towards Europol. Again, the Commission is installing a new, hybrid, centralised body, including for the support of criminal investigations, whilst Europol is already fully competent for CSAM, acting on it through EC3 and through its permanent analysis project Twins. The latter's focus is on the creation and distribution of CSAM through all kinds of online environments, as well as on other online criminal behaviour involving children such as grooming, self-generated indecent material, sexual extortion and live distant child abuse. Moreover, Europol currently already receives large, complex data files including CSAM reports involving European citizens from eg NCMEC, for which the new Europol Regulation (*supra*) now allows big data pre-analysis, whilst the latter has equally enhanced Europol's capacity as a hub to receive multi-jurisdictional data sets directly from private parties such as (OTT) providers.

Customs authorities have traditionally functioned in a hybrid/dual manner, ie through administrative and criminal law cooperation. In the context of the Customs Union, customs authorities have been granted important administrative control, oversight and even sanctioning powers, including for import/export fraud, missing trader intracommunity fraud, customs, excise and VAT fraud, control on the illicit traffic of goods, including precursors, weapons, etc. In their law enforcement capacity, customs authorities have equally been granted adequate cooperation tools (such as the 1997 Naples II Convention), and they may fully rely on Europol, which supports both police and customs authorities in criminal matters. Quite uniquely, both tracks have been smartly connected in quite early an integration phase, ie in the mid-90s, with the setting up of a shared administrative/law enforcement information database, ie the aforementioned Customs Information System (CIS), encompassing a customs File Identification Database (FIDE).

In September 2020, the *von der Leyen* Commission has launched its ideas for the future in a Communication to 'take the Customs Union to the next level'.[12] One of the proposals is to establish a new Customs Agency, for the administrative customs dimension, with more operational powers (*sic*), modelled after the aforementioned (distrust-based) AMLA. The so called Wise Persons Group, set up in September 2021 by the European Commissioner for Economy *Gentiloni* to propose 'innovative' solutions for the most pressing issues faced by the Customs Union, in a report launched in March 2022, calls for a 'moonshot for customs', through the setting up of the said Customs Agency. It should further be able to conduct and benefit from for data-led investigations and risk-based assessments, based on a duty for companies to provide (big) data, and is supposed to facilitate administrative/law enforcement data sharing and to participate in a commonly used data system. Has the Commission forgotten about CIS/FIDE, or about Europol's ability to conduct big data pre-analysis?

[12] European Commission, 'Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Taking the Customs Union to the Next Level: a Plan for Action', COM(2020) 581 final, 28 September 2020 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0581&qid=1605287255064> accessed 31 May 2022.

The Commission seems to have been both strengthening Europol as the primary and all-encompassing EU agency to support and coordinate law enforcement cooperation, by entrusting it new powers and capabilities, and undermining it in parallel through a segmented (and distrust-based) approach of setting up additional central bodies, authorities or centres with competing roles in or towards law enforcement and criminal justice. Within the *(von der Leyen)* Commission, someone, somewhere, someday, ought to think things over, and halt the limitless agentification, for it implies a duplication of efforts, dual structures (top-down, vertical or supranational agencies or authorities juxtaposed to horizontal approaches supported by interconnected databases and support agencies like Europol and Eurojust) and an ensuing fragmented and hybrid approach to crime and 'security' challenges.

Contradictory logics can also be observed when looking at the Commission initiatives, launched in December 2021, on strengthening EU horizontal police cooperation. Whilst, clearly, the Commission is convinced that supranational mechanisms (such as AMLA, JCU, EPPO, the new CSAM Centre, the Customs Agency) are superior to horizontal approaches of agency/database-supported MLA and law enforcement cooperation, it somehow keeps fuelling the latter approaches. In addition to the Europol reform (*supra*), it has proposed several, connected upgrades of horizontal police cooperation (tools) in a police cooperation code, to further operational and information-related cooperation. Its proposed recommendation on operational police cooperation,[13] whilst far from revolutionary, still pushes, among others, for the flexibilization of cross-border hot pursuit and surveillance, the expansion of the use of joint patrols and the turning of Police and Customs Cooperation Centres in border regions into genuine Joint Police and Customs Stations. In the information-related sphere,[14] it has also proposed limited though meaningful steps forward in the further roll-out of the principle of availability (*supra*). Moving to Prüm II is first step. Initial Prüm cooperation (initiated outside the EU and taken over within the EU as from 2008) successfully introduced mutual access to key Member State databases, both full (for vehicle registration data) and hit/no hit based (for fingerprint and DNA databases, making related index data searchable). Prüm II will entail a Prüm router, integrated in the interoperability framework of databases created in 2019, thus allowing fully automated (index) data searches. It will also extend data categories to facial images and introduce a speedier and more predictable hit-follow-up exchange pro-

[13] European Commission,' Proposal for a Council Recommendation on operational police cooperation' COM(2021) 780 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A780%3AFIN&qid=1639134592574> accessed 17 May 2022.

[14] European Commission, 'Proposal for a regulation on automated data exchange for police cooperation ("Prüm II"), amending Council decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' COM(2021)784 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A784%3AFIN&qid=1639141496518> accessed 17 May 2022; European Commission, 'Proposal for a Directive on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA' COM(2021) 782 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A782%3AFIN&qid=1639141440697> accessed 17 May 2022.

cess, through harmonised rules (replacing diverging national rules) and partial automation of this second step of the Prüm process. Europol will also be added as a prosumer in the Prüm framework, making third country-sourced information accessible for automated Member State searches and allowing it, on its turn, to search the Prüm environment (including on behalf of third countries). Member States may further opt-in to making biographical data of suspects and criminals from their national police records indexes equally searchable through an EPRIS (European Police Records Index System) router. Whilst usually too hasty, the Commission is missing both the point and the momentum here. Not only is EPRIS long overdue (called for already by the European Council during the Stockholm Summit of 2008, and prepared by me/my institute in 2012 in consortium with Unisys),[15] the optional nature of EPRIS and the choice to only allow person-based searches is lacking ambition, as if queries on legal persons or objects/events (firearm information, account numbers, telephone numbers, type and date of offence, etc) aren't equally relevant in establishing cross-border connections. The router-based approach is hybrid, in between decentralised and centralised, without data storage at central level. Both the Prüm II and EPRIS central routers would function as a connecting point between Member States' national databases (whilst currently these connect to one another in a fully decentralised fashion). All in all useful/smart but unspectacular upgrades, contrasting with the Commission's eagerness to promote new supranational/vertical initiatives or to bolster centralised horizontal support agencies (like Europol and Eurojust) agencies which it co-controls.

Critically observing and assessing EU criminal policy developments has always been like trying to follow a moving target. The *von der Leyen* Commission's speed booster, however, is not particularly helpful. Academic (let alone democratic) scrutiny has become more difficult than ever. The more, the better, on all fronts, seems to be its motto. Never a dull moment, admittedly. However, steadily and speedily, yet silently, an EU big brother society has been/is being created in just few years' time: interoperability of all sorts of migration and law enforcement databases, a range of new/future hybrid and (semi-)supranational agencies, authorities or bodies, endless series of inter-agency personal data exchange or cross-check possibilities, big data investigations, pre-emptive (AI-based) private screening of reporting and take-down of online content, enhanced monitoring of transactions, etc. The EU's Area of Freedom, Security and Justice may well have been irreversibly reframed in a narrow security logic.

Lastly, since the end of May 2022, also the Russian war in Ukraine is triggering new EU criminal law. Whilst in the initial months after 24 February 2022 the EU's response had already been firm, through strong political and military support to Ukraine, the imposition of economic sanctions against Russia and the freezing of assets of selected Russian and Belarus' targets. End of May 2022, the Commission has tabled a new proposal for a

[15] European Commission, IRCP, Unisys, 'EPRIS: Possible Ways to Enhance Efficiency in the Exchange of Police Records Between the Member States by Setting up a European Police Records Index System', Brussels, 2012, 129 p <https://op.europa.eu/en/publication-detail/-/publication/1301cc77-d7fd-481a-8a63-4d2c5769fc1f> accessed 31 May 2022.

single directive[16] to modernise and bolster the EU's already impressive but scattered legislation on asset recovery and confiscation, which explicitly boosts the Member States' capacity to trace and successfully confiscate assets of individuals and businesses who breach EU sanctions and restrictive measures imposed following the Russian aggression. In parallel, the Commission has further proposed[17] to add sanction evasion and the violation of economic sanctions to the aforementioned Eurocrimes list of Article 83.1 TFEU, which (unlike for LGBTIQ hate speech and hate crime) the Council is expected to swiftly agree to. Last but not least, equally at the end of May 2022, the co-legislators have adopted Regulation (EU) 2022/838,[18] extending Eurojust's role in supporting Member States' action in combating core international crimes (genocide, crimes against humanity and war crimes) and related criminal offences, 'including by preserving, analysing and storing evidence related to those crimes and related criminal offences and enabling the exchange of such evidence with, or otherwise making it directly available to, competent national authorities and international judicial authorities, in particular the International Criminal Court.' Hence, Eurojust, which since 2011 had been hosting the secretariat of the European 'Genocide Network', has now been granted a key role in documenting and preserving battlefield evidence in support of international criminal justice at Member State levels and in the context of the ICC investigation, opened on 28 February 2022.

[16] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation' COM/2022/245 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0245&qid=1653986198511> accessed 25 May 2022.

[17] European Commission, 'Proposal for a Council Decision on adding the violation of Union restrictive measures to the areas of crime laid down in Article 83(1) of the Treaty on the Functioning of the European Union' COM/2022/247 final <https://ec.europa.eu/info/sites/default/files/1_191743_prop_dec_cri_en.pdf> accessed 25 May 2022.

[18] Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences, *OJ* L 148 <https://eur-lex.europa.eu/eli/reg/2022/838/oj> accessed 31 May 2022.

Until the end of the 1990s, EU integration in the area of criminal law centred primarily around the regional deepening of traditional judicial cooperation in criminal matters and the development of law enforcement cooperation (including the setting up of Europol as a support agency). By the end of the 1990s respectively 2000s, the EU also gained (limited) supranational competence in the areas of substantive respectively procedural criminal law. Both judicial and law enforcement cooperation were furthered over the years via the principles of mutual recognition respectively availability, and through the setting up (and development) of Eurojust, the establishment of a European Public Prosecutor's Office and the further development of Europol. After three decennia, the EU criminal law corpus is impressive – a core component of the EU's 'Area of Freedom, Security and Justice', building on and adding to (both real and presumed) trust between the Member States.

No time for stand-still, though. Since 2020, the European Commission has launched a tsunami of new legislative proposals, including in the sphere of EU criminal law, strongly framed in its new EU Security Union Strategy.

This special issue on 'EU criminal policy. Advances and challenges' discusses and assesses some of the newest developments, both in an overarching fashion and in focused papers, relating to key 2022 novelties for Europol (ie the competence to conduct AI-based pre-analysis in (big) data sets, and extended cooperation with private parties), the sensitive debate since 2020 on criminalising (LGBTIQ) hate speech and hate crime at EU level, the 2022 Cybersecurity Directive, the potential of the 2020 Conditionality Regulation to address rule of law issues undermining the trustworthiness of Member States when issuing European Arrest Warrants, and concerns about free speech limitation by the 2021 Terrorist Content Online Regulation.

Gert Vermeulen is Senior Full Professor of European and international Criminal Law and Data Protection Law, Director of the Institute for International Research on Criminal Policy (IRCP), of the Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES) and of the Smart Solutions for Secure Societies (i4S) business development center, all at Ghent University, Belgium. He is also General Director Publications of the AIDP and Editor-in-Chief of the RIDP.

Wannes Bellaert is PhD Researcher and Academic Assistant at the Institute for International Research on Criminal Policy (IRCP), Ghent University.

www.maklu.be
ISBN 978-90-466-1134-0