European Journal on Criminal Policy and Research
https://doi.org/10.1007/s10610-023-09539-9

Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance After the European Investigation Order

Gert Vermeulen[1] · **Martyna Kusak**[2,3]

Accepted: 31 March 2023

Abstract
The purpose limitation principle takes a central place in data privacy law. The specialty principle plays a key role in international cooperation in criminal matters, including in the context of mutual legal assistance (MLA), which is aimed at the cross-border collection and use of information and evidence. Since the specialty principle also frames use limitations for information or evidence obtained through MLA and must therefore be considered a traditional MLA correlative of the purpose limitation principle in data privacy law, both concepts are clearly intertwined. However, since the entry into force of the European Investigation Order, and the EU Data Protection Directive 2016/680 for Police and Criminal Justice, it has become unclear how both principles interplay, and what that implies for the rights position of the data subject or person concerned. This paper unblurs the fuzzy line between specialty and data protection in the current EU MLA context. Based on historical and conceptual analysis, the paper unravels whether the new data protection provisions of the European Investigation Order and Directive 2,016,680 have speciality features and, if so, to which extent they effectively serve a specialty function. This paper does not only demonstrate that both principles do not fully equate with one another, but features an analysis of how they differ, both conceptually and functionally. It argues and concludes that only a fuller, generic specialty rule and data ownership principle have the potential to promote free movement of information and evidence, whilst equally enhancing the procedural rights position of persons concerned.

Keywords Data ownership · European Investigation Order · Law Enforcement Directive 2016/680 · Mutual legal assistance · Purpose limitation · Specialty

✉ Martyna Kusak
m.kusak@amu.edu.pl

Gert Vermeulen
gert.vermeulen@ugent.be

[1] Department of Criminology, Criminal Law and Social Law, Knowledge and Research Platform On Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES), Institute for International Research On Criminal Policy (IRCP), Ghent University, Ghent, Belgium

[2] Faculty of Law and Administration, Adam Mickiewicz University in Poznan, Poznan, Poland

[3] Department Criminology, Criminal Law and Social Law, Institute for International Research On Criminal Policy (IRCP), Ghent University, Ghent, Belgium

Published online: 25 April 2023

Introduction

The specialty rule constitutes a fundamental principle in Council of Europe (hereafter: CoE) and European Union (hereafter: EU) procedures involving the movement (i.e. extradition, surrender or transfer) of persons. It holds that the person concerned may not be proceeded against, sentenced or detained for an offence or act committed prior to his or her extradition, surrender or transfer other than that for which he or she was extradited, surrendered or transferred. The principle is primarily intended to maintain trust between states or authorities involved in such procedures, in that compliance with the specialty rule by the requesting or issuing state prevents the very bypassing of grounds or refusal or non-execution, such as the double criminality requirement or the *ne bis in idem* principle. Its trust-based origin and trust-maintaining function also explain why the requested or executing state may, save in case of *temporarily* transferred persons, authorise exceptions to the specialty rule, by explicitly allowing proceedings, sentencing or sentence execution beyond the original offence or act underlying a person's extradition, surrender or transfer. *Ipso facto*, the specialty principle also protects the person concerned against unexpected or unauthorised actions in the requesting or issuing state, without, however, amounting to a subjective right against actions relating to other prior offences or acts than underlying the original request, warrant or order. As indicated, such actions may, except in case of temporary transfers, be authorised by the requested or executing state, even if the person concerned has not him or herself waived the indirect protection resulting from the specialty rule. The principle, which has only extensively been studied in the context of extradition or surrender procedures (Bassiouni, 2008; Council of Europe, 2006; Lagodny & Rosbaud, 2009; Vermeulen, 2006; Zaïri, 1992), features in both traditional and post-mutual recognition (hereafter: MR) European cooperation instruments relating to movement of persons, by:

- Extradition or surrender, i.e. in Article 14 of the 1957 European Convention on Extradition[1] (hereafter: ECE), Articles 13 and 19 of the 1962 Benelux Extradition and MLA Treaty,[2] Article 66.2 of the 1990 Schengen Implementing Convention (hereafter: SIC),[3] Articles 7–9 and 12 of the 1995 EU Simplified Extradition Convention,[4] Article 10 of the 1996 EU Extradition Convention[5] and Articles 27.2 and 28 of the 2002 Framework Decision on the European Arrest Warrant (hereafter: EAW)[6]
- Temporary transfer of persons in custody in the context of mutual legal assistance (hereafter: MLA), i.e. in Article 11.1 j° Article 12.2 of the 1959 European Convention on Mutual Assis-

[1] European Convention of 13 December 1957 on Extradition, ETS No. 024.

[2] Verdrag van 27 juni 1962 aangaande de uitlevering en de rechtshulp in strafzaken tussen het Koninkrijk België, het Groothertogdom Luxemburg en het Koninkrijk der Nederlanden, Tractatenblad van het Koninkrijk der Nederlanden, 1962, No. 97, Belgisch Staatsblad, 24 October 1967; Traité du 27 juin 1962 d'extradition et d'entraide judiciaire en matière pénale entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas, Mémorial (Journal Officiel du Grand-Duché de Luxembourg) A, No. 13, 22 March 1965.

[3] Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.09.2000, pp. 19–62.

[4] Convention of 10 March 1995, adopted on the basis of Article K.3 of the Treaty on European Union, drawing up the Convention on simplified extradition procedure between the Member States of the European Union, OJ C78, 30.03.1995.

[5] Convention of 27 September 1996 drawn up on the basis of Article K.3 of the Treaty on European Union, relating to extradition between the Member States of the European Union, OJ L C 31, 23.10.1996, p. 12.

[6] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.07.2002, pp. 1–20.

tance in Criminal Matters (hereafter: ECMA),[7] Article 13.6 of the 2001 Second Additional Protocol thereto,[8] Article 9.5 of the 2000 EU MLA Convention[9] and Articles 22.8 respectively 23.3 of the 2014 Directive on the European Investigation Order[10] (hereafter: EIO)

– Transfer of sentenced persons, i.e. in Article 9.1 of the 1970 European Convention on the International Validity of Criminal Judgments,[11] Article 3.4 of its 1997 Additional Protocol[12] (unchanged by the 2017 Amending Protocol thereto[13]) and Article 18 of the 2008 Framework Decision on MR of Custodial Sentences[14]

In stark contrast, very limited conceptual and scholarly attention has been given to the mostly piecemeal and context-specific extension of the speciality rule to the movement *information or evidence through MLA*, though also in this context the principle essentially fulfils the trust-maintaining and indirect protectionist functions as sketched above. It ensures that the requesting or issuing state does not use the information or evidence obtained for the investigation into or prosecution of other offences or acts than underlying its request or order, unless consented to by the requested or executing state or authority. Equally, it provides de facto protection for the suspect or person concerned, which (to some extent) may be waived by the latter (*infra*).

Even where only introduced in the late 1980s (*infra*), the very limited attention for informational or evidential specialty seemed to have completely zeroed out in times of post-MR-based MLA instruments like the EIO, until the matter was unexpectedly raised again during a 2017 European Judicial Network (EJN) Plenary meeting in Tallinn.[15] Member States' authorities were in doubt as to whether evidence obtained through an EIO was subject to the rule of speciality. The Tallinn conclusions did not clarify the problem, but instead highlighted that participants were inconclusive on the matter. In the absence of an explicit general specialty rule in the EIO, some argued that a specialty rule could possibly be derived from Article 19 EIO, stipulating a confidentiality duty for authorities involved. Others advocated that, based on the mere fact that an EIO is issued with respect to specific criminal proceedings,[16] the use of EIO-obtained evidence should not automatically be allowed in other proceedings, in which certain grounds for

[7] European Convention of 20 April 1959 on Mutual Assistance in Criminal Matters, ETS No. 30.

[8] Second Additional Protocol of 8 November 2001 to the European Convention on Mutual Assistance in Criminal Matters, ETS No. 182.

[9] Convention of 29 May 2000 established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, pp. 3–23.

[10] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1–36.

[11] European Convention of 28 May 1970 on the international validity of criminal judgments, ETS No. 070.

[12] Additional Protocol of 18 December 1997 to the European Convention on the transfer of sentenced persons, ETS No. 167.

[13] Protocol of 22 November 2017 amending the Additional Protocol of 18 December 1997 to the European Convention on the transfer of sentenced persons, CETS No. 222.

[14] Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, OJ L 327, 5.12.2008, pp. 27–46, as amended by Framework Decision 2009/299/JHA of 26 February 2009, OJ L 81, 27.3.2009, pp. 24–36.

[15] Extract from the Conclusions of the 49th Plenary meeting of EJN, https://www.ejnforum.eu/cp/registry-files/3373/ST-15210-2017-INIT-EN-COR-1.pdf n.d., p. 9.

[16] See in the same sense: Sjöcrona, 1990, p. 158, wondering whether it should be implicitly supposed that the Dutch legislation determines a condition of speciality based on the fact that Article 552 h Dutch Code of Criminal Procedure stipulates that a request for minor legal assistance is being done in connection with a *criminal case* (italics added).

non-execution of an EIO might have been invoked. It was also stated that 'apart from its specific role in extradition and transfer of sentenced persons matters, the "rule of speciality" traditionally applies also to rogatory letters for gathering evidence', for which support was sought in Article 23 EU MLA Convention, pertaining to data protection. The pragmatic 'solution' put forward in the conclusions was to clarify the ambiguity on a case-by-case basis, by seeking the authorisation of the executing Member State's authorities, preferably by using an EIO form, before using any EIO-obtained evidence beyond its initial purposes.

The issue has too much practical, conceptual and *principled* importance to leave it underexplored and to not unblur the fuzzy line between specialty and data protection in the current EU MLA context, i.e. after the EIO. Hence, this article unravels how speciality and data protection rules interplay, i.e. whether data protection provisions have speciality features (first sub-question) and, if so, to which extent they effectively serve a specialty function when using an EIO (second sub-question). It concludes that only a fuller, generic specialty rule has the potential to promote free movement of information and evidence, whilst equally enhancing the procedural rights position of persons concerned. Before fully embarking on these focused discussions, it is key to map and study the *piecemeal* introduction of the specialty principle as a *use* limitation for information and evidence gathered through MLA on CoE and EU levels, in order to better understand the context-specific reasons for such recognition and the organic interplay with data protection and to better grasp the possible merits of a fuller, generic specialty principle for movement of information or evidence.

Speciality as a Use Limitation for Information or Evidence Gathered Through MLA[17]

Council of Europe

Notwithstanding the fact that the 1959 ECMA does only[18] feature a specialty rule for the temporary transfer of persons in custody (*supra*), informational or evidential speciality seems to play a certain role in day-to-day MLA between the Parties, with a (limited) number of EU Member States having explicitly valued the principle in this context.[19] Mostly, however, they have not made a reservation to the ECMA in this respect. This presupposes that they do execute letters rogatory in their territory and carry out investigations as requested, only expressly *asking* that the information or evidence obtained is not used

[17] Largely based on and updated from: Vermeulen, 1999, pp. 112–123 and the literature quoted therein.

[18] On the fact that according to the ECMA the speciality principle should not be respected in the context of MLA, see historically inter alia: Vogler, 1985.

[19] As appears from the answers of the then 15 Member States to the questionnaire on MLA (*Conseil de l'Union européenne*, 8488/95, *Note de la future présidence espagnole au Groupe "Criminalité organisée internationale": Projet de questionnaire sur l'entraide judiciaire en matière pénale*, 26 June 1995, 5; 10,198/95, *Note du Secrétariat Général du Conseil au Groupe "Entraide judiciaire en matière pénale": Questionnaire sur l'entraide judiciaire dans les matières pénales (Télex n° 3195 du 27 juillet 1995) – Réponses des* délégations, 7 November 1995, 21), sent in mid-1995 by the Spanish Presidency in the aftermath of the Bordeaux Seminar, held on 20–22 April 1995 on the initiative of the French Presidency (*Conseil de l'Union européenne*, 7193/95, *Note de la Présidence en date du 16 mai 1995 au Groupe Directeur III: Séminaire d'entraide judiciaire organisé par la Présidence française à Bordeaux du 20 au 22 avril 1995,* JUSTPEN 72, 16 May 1995, 2). Member Sates indicating they adhered to the specialty rule were Germany, Greece, Spain, Luxembourg, Portugal and Sweden. In addition, Ireland has, in its instrument of ratification to the ECMA of 28 November 1996, expressed a reservation of speciality with Article 2 ECMA.

without their consent for purposes other than contained in the MLA request, i.e. in the context of other proceedings than those for which MLA has been granted. However, in the absence of a reservation in this respect,[20] they do not appear to be able to impose a genuine speciality condition.

This ambiguity prompted the CoE to gradually introduce a speciality principle in MLA for information or evidence gathering purposes, be it only for very specific contexts or specific forms of MLA.

In Recommendation R(85)10, relating to the practical application of the ECMA with regard to letters rogatory for the interception of telecommunications,[21] the Committee of Ministers prioritised enabling the requested state to carry out requests to monitor telecommunications only under the condition that the evidence obtained by means of the monitoring measure would not be used for purposes other than those for which the legal assistance was requested and granted (Article point 4.d of the annex to the Recommendation). By stipulating in the Recommendation that information which the requesting state would obtain regarding offences other than those for which bugging or tapping measures had been requested ought not to be used in investigations, prosecutions or proceedings relating to such other offences, the CoE framed its first *soft law* speciality rule in the sphere of information or evidence gathering. Over time, it has also introduced such conditions in several of its conventions.

A first *hard law* possibility for stipulating specialty conditions was inserted in the 1990 Money Laundering Convention[22] (Article 32) (continued in the 2005[23] edition, Article 42). According to the provision(s) concerned, the requested Party may make its execution of a request subject to the condition that the information or evidence obtained will not, without its prior consent, be used or transmitted by the authorities of the requesting party for investigations or proceedings other than those specified in the request. Such trust-maintaining provision had a double function, specific to the money laundering context: (1) whilst certain countries wanted a grindle to bar the use of financial information provided beyond criminal proceedings, e.g. for administrative/fiscal investigations, (2) the early days of anti-money laundering instruments were still marked by a significant degree of national discretion to only recognise money laundering for a limited, and varying, set of predicate offences. In the initial stages of money laundering investigations, it is often impossible to ascertain from which crime or predicate offence the funds involved have allegedly been derived, so that requiring double criminality would have plainly frustrated the possibility of MLA in early money laundering investigations. The choice to allow for an informational/evidential specialty condition was an alternative offering the same guarantees, be it in a later stage, i.e. after the predicate offence has been ascertained (Stessens, 2000, pp. 195, 272).

Speciality was also introduced in a piecemeal fashion, i.e. for certain forms of MLA only, in the 2001 Second Additional Protocol to the ECMA.[24] In the draft Protocol, it had been proposed

[20] In addition to Ireland (instrument of ratification deposited on 28 November 1996), also the following non-EU states have entered a specialty reservation in connection with Article 2 ECMA: Andorra (instrument of ratification deposited on 26 April 2005), Monaco (instrument of ratification deposited on 19 March 2007), San Marino (instrument of ratification deposited on 18 March 2009) and Switzerland (reservation amended by letter registered on 13 December 1996).

[21] https://rm.coe.int/09000016804e6b5e, access: 1.06.2019.

[22] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, European Treaty Series No. 141 n.d..

[23] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Council of Europe Treaty Series No. 198 n.d..

[24] Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, European Treaty Series No. 182.

that the requested state would be enabled to impose a wide-ranging and generic speciality condition, in that use of the information or evidence provided would not be allowed in the context of investigations or proceedings for which the requested state could have refused legal assistance in pursuance of the ECMA. However, this rule was not inserted into the Protocol's final version. Instead, the Protocol only allows (limited) specialty for spontaneously provided information (under Article 11, drawing inspiration from Article 7 EU MLA Convention) and provides detailed conditions for the use of information lawfully obtained by a member or a seconded member of a joint investigation team (hereafter: JIT) where the information concerned is not otherwise available to the competent authorities of the states concerned (under Article 20.10 Protocol, drawing inspiration from Article 13.10 EU MLA Convention). According to this article, subsequent use is allowed for the four limited purposes laid down in the article.[25] Another provision which, to a certain extent, fulfils a speciality function is Article 26 of the Protocol, relating to data protection. This article was largely copied from Article 23 EU MLA Convention, which is discussed fuller later in this article (*infra*, under 2.3). Article 26 stipulates that personal data transferred from one Party to another as a result of the execution of a request made under the ECMA may be used by the Party to which such data has been transferred only: (a) for the purpose of proceedings to which the ECMA or any of its Protocols apply; (b) for other judicial and administrative proceedings directly related to the proceedings mentioned under the previous condition; and (c) for preventing an immediate and serious threat to public security. Moreover, the use of such data for *any* other purpose is allowed if prior consent to that effect is given by either the state from which the data will be transferred or the data subject.[26] Moreover, any party that transfers personal data obtained as a result of the execution of a request may require the state to which the data has been transferred to give information on the use made of such data.[27]

The 2001 Cybercrime Convention[28] provides yet another example. According to Article 28.2,[29] the requested party may make the supplying of information or material in response to a request dependent on the condition, among others, that it will not be used for investigations or proceedings other than those stated in the request. Hence, when responding to a request for mutual assistance, the requested party may impose the speciality condition. As the Explanatory Report to the Convention states, 'in order for this condition to apply, it must be expressly invoked

[25] (1) For the purposes for which the team has been set up, (2) subject to the prior consent of the Party where the information becomes available, for detecting, investigating and prosecuting other criminal offences, whereby consent may be withheld only in cases where such use would endanger criminal investigations in the Party concerned or in respect of which that Party could refuse mutual assistance, (3) for preventing an immediate and serious threat to public security, and without prejudice to sub-paragraph b. if subsequently a criminal investigation is opened and (4) for other purposes to the extent that this is agreed between Parties setting up the team.

[26] Only 19 out of 41 ratifying states made a reservation to this article.

[27] When comparing this final approach to the draft protocol, it is notable that speciality has changed its meaning in the context of MLA. The draft proposal was both broad and strict: firstly, it related to the *information* and *evidence* (without the requirement of lawfulness), which covers all the possible outcomes of legal assistance; secondly, the further use of such information and evidence was limited to cases in which the ECMA would apply between the parties; and thirdly, it did not provide exceptions, such as involved parties' consensus. In contrast, the final version distinguishes between 'information lawfully obtained' (in the context of JITs) and 'personal data', meaning not all information and evidence are subject to speciality, but only those which belong to one of these clusters.

[28] Council of Europe, Convention on Cybercrime, European Treaty Series No. 185 n.d..

[29] See the Explanatory Report: 'This provision specifically provides for limitations on use of information or material, in order to enable the requested Party, in cases in which such information or material is particularly sensitive, to ensure that its use is limited to that for which assistance is granted, or to ensure that it is not disseminated beyond law enforcement officials of the requesting Party. These restrictions provide safeguards that are available for, inter alia, data protection purposes', ETS No. 185, p. 49.

by the requested party, otherwise there is no such limitation on use by the requesting party. In cases in which it is invoked, this condition will ensure that the information and material may only be used for the purposes foreseen in the request, thereby ruling out use of the material for other purposes without the consent of the requested party'.[30] Also in this context, the choice to allow for specialty conditions can be explained by the specific cybercrime context, in which e.g. no agreement could be found on including racist propaganda among content-related offences (Csonka, 2006: 487), thus requiring extra prudence in the shape of a specialty.

EU

The EU approach to informational or evidential speciality in MLA has been equally piecemeal and ad hoc, limiting the principle to specific contexts or forms of cooperation only.

A cross-border speciality rule was, for the first time, inserted in Article 50.3 SIC, which later was integrated in the EU framework as part of the Schengen *acquis*. Its function was very specific. In Article 50.1, the Parties had agreed to a limitation of the traditional fiscal offence exception, by accepting to grant one another MLA also in the sphere of *indirect* tax, i.e. for infringements of their laws and regulations on customs and excise duties and VAT. For Luxembourg, as one of the five initial Schengen countries, this constituted a historic breakthrough, both in its relations with France and Germany under the ECMA and with Belgium and the Netherlands under the 1962 Benelux Extradition and MLA Treaty. In order to prevent possible bypassing of the fiscal offence exception, Luxembourg required a guarantee that information or evidence provided under Article 50.1 would not later be used in cases of *direct* taxation, i.e. pertaining to income tax. Hence, a tailor-made and context-specific trust-maintaining rule was laid down in Article 50.3, according to which the requesting Party shall not forward or use information or evidence obtained from the requested Party for investigations, prosecutions or proceedings other than those referred to in its request without the prior consent of the requested Party, thus making sure that Luxembourg would be able to invoke the traditional fiscal (or even *ordre public*) exception whenever use beyond indirect tax would be envisaged or possible. Interestingly, this early SIC specialty rule did not only prohibit use by the requesting Party of the information or evidence for purposes other than those indicated in its request, but also onward transmission by it without the prior assent of the requested Party.

A context-specific trust-maintaining guarantee was also inserted in the Naples II Convention.[31] Article 23.3 provides that, if in the course of a covert investigation information is acquired in relation to an infringement other than covered by the original request, the use conditions for such shall also be determined by the requested authority in accordance with its national law. This speciality rule finds its basis in the persisting national sovereignty claim of the Member States over sensitive investigative methods like covert investigations when used across borders.

Such *locus regit informationem* rule for sensitive methods did not generically make it in the later EU MLA Convention, even if similar distrust was obviously underlying the choice made therein to maintain the *locus regit actum* principle for JITs, controlled deliveries and covert investigations, notwithstanding a general shift to *forum regit actum* in the execution of MLA requests. Only for spontaneous information exchange, for information lawfully obtained within a JIT and for interception of

[30] Explanatory Report to the Convention on Cybercrime, p. 50.

[31] Convention drawn up on the basis of Article K.3 of the Treaty on European Union on mutual assistance and cooperation between customs administrations, OJ C 24, 23.01.1998, pp. 2–22 n.d..

telecommunications a true speciality rule was built in. As for the new possibility of spontaneous information exchange, which had already been introduced at EU level for customs cooperation and, through Article 46 SIC, for police cooperation, Article 7.2 EU MLA Convention phrased a clear-cut specialty rule, mirroring the default *data owner principle* underlying information exchange under the Europol Convention.[32] Until date, the latter has been key in shaping and maintaining trust between the Member States' law enforcement authorities in sharing information,[33] including under the 2009 Europol Decision[34] and the 2016 Europol Regulation[35] regimes. In addition, Article 13.10 EU MLA Convention makes the use of new information lawfully obtained by a (seconded) JIT member for detecting, investigating and prosecuting other criminal offences than those for which the JIT has been set up subject to the prior consent of the Member State in which the information has become available. For the scenario of interception of telecommunications on its territory and the immediate, so-called real-time transmission thereof to the requesting Member State, as foreseen in Article 18.1, under (a) EU MLA Convention, the requested Member State may, according to Article 18.5, under (b), make its consent subject to any conditions which would have to be observed in a similar national case, i.e. including *use* conditions. According to Article 18.6, the same goes for the scenario of interception, recording and subsequent transmission—the so-called non-real-time interception—as foreseen in Article 18.1, under (b) EU MLA Convention. This optional specialty rule was, moreover, taken over in full in Article 30.5 EIO. Equally for all scenarios of remote or continued interception of the telecommunications of a person specified in an interception on a Member Sate's territory from which no technical assistance is needed to carry out the interception, *use* specialty was guaranteed in the EU MLA Convention. According to Article 20.4, under (a)(iii), the latter Member State may require that any material already intercepted whilst the person concerned was on its territory may not be used or may only be used under conditions which it shall specify. The EIO, once again, has continued this specialty option in Article 31.3, under (b).

A generically applicable specialty rule was, however, never introduced in the EU MLA landscape. On the contrary,[36] in the negotiations on the later 2000 EU MLA Convention, the point of view was adopted that the speciality requirement should be abandoned as

[32] Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office, OJ C 316 of 27 November 1995.

[33] Europol, Data Protection Office (2011). *Data Protection at Europol.* Publications Office of the European Union, https://doi.org/10.2813/38585, 19; Drewer, D. & Ellermann, J. (2012). Europol's data protection framework as an asset in the fight against cybercrime. *ERA Forum* 13, point 4; Europol (2013). *EIS. Europol Information System. Crime reference system for EU law enforcement and cooperation partners.* Publications Office of the European Union, QL-32–13-058-EN-D, p. 2; Council of the European Union (2016). *Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area*. 9368/1/16 REV1; pp. 12–13, 26–27 and 41.

[34] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office, OJ L 121 of 15 May 2009.

[35] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135 of 11 May 2016.

[36] And counter to the then trend to give the principle a permanent—and formal—place in MLA. The speciality principle had been gaining importance in the context of MLA, even as a generic principle, as confirmed in: Orie et al., 1991, p. 110; Rozie, 1996, p. 64.

much as possible. The Member States' approaches to the issue had been examined in a questionnaire on MLA, sent to all Member States in mid-1995,[37] in which they had been explicitly asked whether a speciality condition applied (under their domestic law) with respect to information passed onto another state in connection to criminal registers or the execution of sentences, summonses or other procedural documents. The questionnaire aimed to identify whether use by the requesting Member State of the said information should be allowed in investigations or matters other than those relating to the acts for which MLA had been requested. Questions also featured as to possible difficulties that would arise in the Member States' domestic legislation in case no specialty rule would be inserted. Interestingly, the majority of delegations indicated that no specialty rule had been laid down in their domestic legal order, whilst a generic specialty principle had neither been framed under the ECMA or the Benelux Extradition and MLA Treaty. Consequently, they saw no reason to consider the matter any longer, and no specialty rule was laid down in the new Convention, save for a specialty option as part of the conditions to which interception of communications could (and can) be subjected (*supra*). With scattered, context-specific specialty rules, i.e. in SIC (for indirect tax matters), in Naples II (for covert investigations) and in the EU MLA Convention (for spontaneous information exchange, newly obtained JIT-information and interception of communications), the EU specialty approach was fragmented, and not quite coherent.

At the same time, however, the drafters of the 2000 EU MLA Convention took an innovative step, incorporating rules on the protection of personal data communicated under the Convention in Article 23 (used in 2001 by the CoE as the basis for Article 26 of the Second Additional Protocol to the ECMA). Article 23 introduced purpose limitation for information or evidence containing personal data. According to the Convention and its Explanatory Report, the purpose for which personal data may be used dictates the conditions in which it may be used, i.e. in some cases without and in other only with the prior consent of the Member state that has forwarded the data. According to Article 23.1, the recipient Member State may use information without the prior consent of the providing Member State in three cases, i.e. (a) for the purpose of proceedings to which the Convention applies, (b) for other judicial and administrative proceedings directly related to such proceedings and (c) for the purpose of preventing an immediate and serious threat to public security. As regards the use of personal data for 'any other' purpose, paragraph 1 (d) stipulates that the Member State wanting to use it must obtain the prior consent of the supplying Member State supplying it, unless the former Member State has obtained the consent of the data subject.

Although Article 23 of the EU MLA Convention relates to *only* personal data communicated under the Convention, it is not *solely* a data protection provision, but a hybrid construct with both data protection and speciality features. Even if the provision is unambiguously aimed at protecting personal data in an MLA context and does not protect against the bypassing of possible grounds for refusal or of certain domestic rules of the requested Member State (as *supra* in the case of covert investigations or interception

[37] *Conseil de l'Union européenne*, 8488/95, *Note de la future présidence espagnole au Groupe "Criminalité organisée internationale": Projet de questionnaire sur l'entraide judiciaire en matière pénale*, 26 June 1995, 5; 10,198/95, *Note du Secrétariat Général du Conseil au Groupe "Entraide judiciaire en matière pénale": Questionnaire sur l'entraide judiciaire dans les matières pénales (Télex n° 3195 du 27 juillet 1995) – Réponses des* délégations, 7 November 1995, 21), sent in mid-1995 by the Spanish Presidency in the aftermath of the Bordeaux Seminar, held on 20–22 April 1995 on the initiative of the French Presidency (*Conseil de l'Union européenne*, 7193/95, *Note de la Présidence en date du 16 mai 1995 au Groupe Directeur III: Séminaire d'entraide judiciaire organisé par la Présidence française à Bordeaux du 20 au 22 avril 1995,* JUSTPEN 72, 16 May 1995, 2).

of telecommunications), it has undeniably certain specialty characteristics. Firstly, Article 23 qualifies as a historic framing of the integrity of MLA in criminal matters on a meta level: the later surpassing of its criminal justice purpose must be avoided, except in three 'acceptable' situations, i.e. for (1) so-called administrative offences,[38] (2) for certain connected procedures, even other than in criminal matters (*infra*) and (3) for the purpose of preventing an immediate and serious threat to public security (again building on the SIC *acquis*).[39] In doing so, Article 23 functions as the first *general* personal information-related specialty clause in MLA, be it that use limitations are not framed on the level of specific offences (like indirect tax offences) or for specific forms of cooperation (like covert investigations, spontaneous information exchange, JITs or interception of telecommunications), but on the level of a (widely defined) criminal justice purpose. The value thereof for judicial cooperation cannot be underestimated (Vermeulen, 2011a, 2011b; Vermeulen & Ryckman, 2012: 102–103), especially not in terms of limiting the ever-growing blurring of criminal justice and public or national security purposes that we have been witnessing since, both in the context of fighting terrorism and managing the migration crisis,[40] and which has even permeated into the Data Protection Directive 2016/680 for Police and Criminal Justice (hereafter: LED).[41] Secondly, Article 23 also radically diverts from the commonly accepted and well-known contemporary data protection perspective, as enshrined inter alia in the LED (recitals 35 and 37), which excludes reliance on the data subject's consent as an autonomous legal ground for the processing of personal data by judicial or law enforcement authorities, arguing that consent can never be 'freely given' in such context, due to an inherent imbalance in power in the relationship between the data subject and the data controller (Leiser & Custers, 2019;

[38] A historical *acquis*, finding its origin in the German *Ordungswidrigkeiten*, generically accepted since Article 49 (a) SIC and further widened by Article 3.1 EU MLA Convention.

[39] Reference should me made here to Article 46.1 SIC, allowing the use of spontaneously transmitted police information to 'prevent […] threats to public policy and public security', as well as to various SIS-related provisions, both pertaining to alerts on foreigners to be refused entry (Article 96: which 'may be based on a threat to public policy or public security or to national security which the presence of an alien in national territory may pose') and to the overall SIS purpose (Article 93: 'to maintain public policy and public security, including national security') and especially its general data protection-related purpose limitation (Article 102.3: 'any derogation from paragraph […] must be justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security').

[40] On the generalised law enforcement (or judicial) access to or use possibilities of immigration-related EU information systems: Vavoula, 2017. Note that both 2019 interoperability Regulations have institutionalised purpose blurring between criminal justice and migration spheres (Regulation (EU) 2019a/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135 of 22 May 2019; Regulation (EU) 2019b/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135 of 22 May 2019).

[41] 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, OJ L 119, 4.05.2016, pp. 89–131. The directive is commonly referred to as the 'the law enforcement directive' (abbreviated 'LED').

Sajfert & Quintel, 2020).[42] The express possibility in Article 23.1, under (d) (which has also been copied by the CoE into Article 26 of the Second Additional Protocol to the ECMA), is reflective as well of its hybrid nature: the ability for the person concerned to agree to the surpassing of initial purpose limitations by the requesting state finds it origin in the specialty principle as it has developed in the context of extradition, surrender or the transfer of persons (*supra*), where the possibility for the person concerned to impact the otherwise inter-state or inter-authority cooperation process in criminal matters has only slowly made its way in. Cooperation in criminal matters had traditionally been a context in which the person concerned was only the *object* of cooperation instead of its *subject*, i.e. a person with its own voice and its own interests, gradually being entitled certain subjective rights, such as the right to be heard or even the right to object, the rights to legal remedies, the right to be assisted by a lawyer, the right to ask for investigative measures *à décharge* or even the right to ask to not invoke grounds for refusal when deemed against its interest. Against this backdrop, the recognition by Article 23 that use of information beyond its initial purpose may be allowed based on the consent of the data *subject* functions as an extra guarantee (Vermeulen, 2019)[43] in that the person

[42] 'As regards the basis for the lawfulness of processing, the Directive lays down only one legal ground in Article 8 (if necessary for the performance of a task carried out by a competent authority for the purposes of the Directive and based on Union or Member State law), while Article 6 of the GDPR provides for six different legal bases. Obviously, the legislator recognized that LEAs may only carry out tasks permitted by law, and not process data for the purposes of the Directive on the basis of consent […]'. The above LED-specific doctrine is in line with the post-GDPR interpretation of valid 'consent', as initially elaborated by the WP29 (Guidelines on Consent under Regulation 2016/679 (wp259), adopted on 28 November 2017 and revised on 10 April 2018) and later the EDPB (Guidelines 05/2020 of 4 May 2020 on consent under Regulation 2016/679, version 1.1), which rightfully warn against possible abusive (and hence: inacceptable) reliance on consent in relations in which the data controller holds a position of authority or power vis-à-vis the data subject, which is indeniably the case when the latter is confronted with police or law enforcement authorities. Note, however, that, before the explicit exclusion in the recitals of the LED, no hard law prohibition to rely on the data subject's consent for data processing by judicial or law enforcement authorities has been framed. At best, such prohibition could fairly implicitly – and, moreover, only for the police and not for judiciairies – be derived from the wording of principle 2.1 of CoE *non-binding* Recommendation No. R(87) 15 of the Committee of Ministers to Member States on regulating the use of personal data in the police sector, in that the '[t]he collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation'. Also the newly adopted 2018 CoE Practical Guide on the use of personal data in the police sector (T-PD(2018)01) remains silent on the matter, just like the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108, as amended by Protocol of 10 October 2018, Council of Europe Treaty Series, No. 223) or the Explanatory Report to it. It can also be noted that certain European countries, like the UK (notwithstanding the fact that it was bound by the LED in the pre-Brexit phase and that its relations with the EU remain to be governed by the LED principles following the adoption by the European Commission on 28 June 2021 of Adequacy Decision C(2021)4801 final, under Article 36 LED), do allow for the processing of personal data for law enforcement purposes if based on law and where 'the data subject has given consent to the processing for [such] purpose' (Sect. 35(2)(a) UK Data Protection Act 2018), with the possibility of 'the processing [being] necessary for the performance of a task carried out for [such] purpose by a competent authority' constituting only an alternative option (reflected in Sect. 35(2)(b)).

[43] Confirmed in: Consultative Committee of The Convention For The Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Opinion on the provisional text and explanatory report of the draft Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data, T-PD(2019)8FIN, Strasbourg, 20 November 2019, p. 10, footnote 1.

concerned may deliberately want such use,[44] whilst the requested or executing state or authorities see no interest in allowing it. It marked the first recognition of a *subject*-triggered stretching of the specialty rule as an *informational* use limitation, be it limited in scope to the use of the data subject's own personal data. All of the other above-analysed legal instruments (the Money Laundering Convention, the Second Additional Protocol to the ECMA (as for Article 20.10), the Cybercrime Convention, the SIC, or the Naples II Convention) allowed use of information or evidence beyond the initial or context-specific purpose solely after prior consent of the requested state, i.e. above the head of the person concerned. Article 23.1 under (d) EU MLA Convention combines both data protection and specialty functions in a flexible manner. It also introduces a high standard of protection by allowing the data subject a voice in the control process over the use of its data, which otherwise would be left to the sole discretion of the requested or executing state or authority.

The piecemeal attention for informational or evidential specialty has completely zeroed out in times of post-MR-based MLA instruments like the EIO, without explanation why the application of speciality would no longer be of relevance in this context. This approach seems to underestimate the trust-maintaining and indirect protectionist function of speciality. The MR-based form of cooperation can only thrive on an enhanced level of mutual trust which turned out to have more political than genuine foundations. The numerous grounds for non-recognition and non-execution also in post-MR instruments, as well as specific provisions of the EIO (such as Article 10, Article 11.1(f), Article 11.1 (h)), do not, however, act as examples of enhanced mutual trust. Against this backdrop, in the specific context of the EU mutual recognition cooperation instruments, a fuller specialty rule would be beneficial—as a cornerstone for the trust required for free movement of information and evidence in the EU criminal justice.

Speciality in the EIO?

Data Protection and Informational Specialty: Correlatives, yet not Interchangeable

Even if Article 23 EU MLA Convention has outspoken specialty features that strongly interplay with its primary data protection function, data protection and informational or evidential specialty certainly do not fully equate with one another. Personal data must be lawfully and fairly collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible therewith. Whilst the specialty principle also firms use limitations for information obtained through MLA and must therefore be considered a traditional MLA correlative of the purpose limitation principle in data protection law, both concepts are surely not interchangeable.

Firstly, the informational or evidential specialty principle extends beyond personal data. Secondly, it allows the data subject in criminal matters a stronger position than according to

[44] On the importance of a possibility to surpass limitations and (even mandatory) refusal grounds upon the express request of the defence or person concerned, see: Sjöcrona, 1990, pp. 58–59, quoting also Nagel: "*Es liegt also nahe, eine flexibelere Handhabung der Kriterien für die Fälle vorzusehen, in denen es um die Erhebung von Entlastungsbeweisen geht*" (Nagel, 1988, p. ?); Commissie tot bestudering van de positie van verdachten en andere belanghebbenden in de internationale strafrechtelijke samenwerking, 1993, p. 56; Vermeulen et al., 2002, pp. 26, 134–135. The latter have even proposed a fully-fledged provision on the matter in their draft Belgian code of international cooperation in criminal matters.

data protection law, even if data protection is a subjective (fundamental) right, unlike specialty protection. Thirdly, and foremost, the purpose limitation dimension of the specialty rule has a trust-shaping and trust-maintaining function on an inter-state or inter-authority level. Its goal in information-related or evidence-related judicial cooperation is to prevent the very bypassing of grounds for refusal or non-execution,[45] which, notwithstanding MR, have remained numerous in contemporary EU MLA. In a law enforcement context (such as on a Europol level), this function has even translated into the so-called data owner principle (*supra*), whereby, in the absence of grounds for refusal (law enforcement information exchange being largely non-mandatory),[46] compliance with use limitations set by the providing law enforcement authority constitutes the very trust foundation of cooperation.

The key question for the future is whether MR, which can only thrive on an enhanced level of mutual trust, can afford not to have specialty or data ownership.

Article 23 EU MLA Convention and the Tallinn Dilemma

Unlike the failed European Evidence Warrant,[47] which was meant to simply coexist with the EU MLA Convention,[48] the EIO, which does envisage to replace the corresponding provisions of the latter Convention, initially featured an autonomous data protection provision (Article 20). It took the form of a simple reference to Framework Decision 2008/977/JHA,[49] as well as to the 'principles' of the CoE Convention for the protection of individuals with regard to Automatic Processing of Personal Data of 28 January 1981[50] and its Additional Protocol.[51] Since framework Decision 2008/977/JHA has in the meantime been repealed by the LED, art. 20 EIO has been deleted accordingly,[52] and the LED henceforth

[45] See already in the pre-EU era: Orie, 1986, p. 177: 'with the absence of [the] speciality principle the barriers in the legal assistance law, the grounds of refusal, lose a great deal of their significance'.

[46] Unless under the so-called Swedish Framework Decision (Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, pp. 89–100), which introduced, in Article 3, the first *obligation* to provide information or intelligence in a EU cross-border law enforcement context.

[47] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, 30.12.2008, pp. 72–92.

[48] Article 21 stipulated that the Framework Decision would 'coexist with existing legal instruments in relations between the Member States in so far as these instruments concern mutual assistance requests for evidence falling within the scope of [the] Framework Decision'.

[49] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, pp. 60–71.

[50] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108 n.d..

[51] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, European Treaty Series No. 181 n.d..

[52] Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, OJ L 39, 21.02.2022, pp. 1–3.

constitutes the main framework for the processing of personal data gathered using the EIO, but, apparently, not the sole. This is due to Article 34 EIO directive, according to which, as already stated above, the EIO replaces the 'corresponding' provisions of selected conventions applicable between the Member States bound by it, including, among others, the EU MLA Convention.[53] Hence, the key question is whether the LED can or must be considered a truly 'corresponding' provision with Article 23 EU MLA Convention. The answer requires a fuller and more substantial assessment.

In doing so, it immediately strikes that the LED takes a different and stricter approach than the EU MLA Convention in setting the purposes of personal data processing. Article 23 of the Convention allows processing (a) for the purpose of proceedings to which the Convention applies, (b) for other judicial and administrative proceedings directly related to such proceedings, (c) for the purpose of preventing an immediate and serious threat to public security and (d) even for any other purpose, based on the consent of either the requested Member State or the data subject. Unlike the Convention, the LED is specific for international cooperation procedures and generically limits processing by competent authorities to the purposes of 'prevention, investigation, detection or prosecution of criminal offences or [of] execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Article 2.1 j° 1.1), moreover introducing an additional purpose limitation test in the case of processing by the same or another controller for any of such purposes (i.e. those listed under Article 2.2 j° 1.1 LED) other than that for which the personal data have originally been collected (Article 4.2 LED).[54] Even if we will only run a fuller comparison between both frameworks below (*infra*, under 4), it is obvious that the MLA Convention is much more flexible than the LED, e.g. by allowing possible use for 'any' purpose and by its allowance to rely on the data subject's consent (*supra*). Article 34 EIO is unclear about what should happen where its provisions only correspond 'in part' with predecessor provisions. It seems fair to opt for a narrow interpretation. That leads us to the preliminary conclusion that Article 23 EU MLA Convention does not fully correspond to the LED which applies to the EIO, so that at least its non-corresponding elements or sub-provisions (if feasible to separate from the corresponding ones) continue to apply in post-EIO context, or that it continues to apply altogether.

The last scenario, according to which Article 23 of the Convention still applies in full, is plainly supported by Article 60 LED, according to which the EU's specific provisions for the protection of personal data in the field of judicial and police cooperation in criminal matters that have entered into force before the transposition of the LED remain unaffected.[55] This chronological argument leaves no doubt as to the continued application of Article 23 of the MLA Convention. Recital 94 LED is

[53] Other conventions are the ECMA, as well as its two additional protocols and the bilateral agreements concluded pursuant to Article 26 thereof and the SIC.

[54] According to Article 4.2 LED, such change of purpose, even if staying within the boundaries of the purposes allowed under Article 2.1 j° 1.1 LED, will only be permissible under the following cumulative conditions: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

[55] Article 60 LED: 'The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected'.

even explicit: 'Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to […] *Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*' [italics added].

In conclusion, the EU MLA Convention regime remains unaffected. Not only do its specialty-inspired limitation of permittable cross-over between criminal justice and national security purposes and allowance to rely on the data subject's consent find no 'correspondence' in the LED, the latter even unambiguously confirms the continued applicability of Article 23 of the Convention in a post-LED (and therefore post-EIO) context.

The Tallinn dilemma is hereby solved: information or evidence obtained through an EIO is not subject to a genuine specialty rule. Specialty was never generically introduced in information-related MLA, and neither has the EIO introduced it. The EIO only features an optional informational or evidential specialty rule in a single context, i.e. the interception of telecommunications, for which Articles 30.5 and 31.3, under (b), continue to allow the Member State where the data subject is communicating to stipulate use conditions. In addition, Article 23 EU MLA Convention continues to apply, with its specialty features, but without amounting to a generic specialty principle.

In Cauda Venenum?

Article 23 EU MLA Convention, hybrid as it is, probably only has a single, but manifest substantive weakness, i.e. that its accepted use purposes are endlessly stretchable (for 'any' purpose) based on the prior consent of the requested Member State (Article 23.1, under (d)). That is not in accordance with the LED, which limits overall data processing by competent authorities to purposes of 'prevention, investigation, detection or prosecution of criminal offences or [of] execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Article 2.1 j° 1.1).

The strengths of the MLA Convention regime, however, are multiple, and at risk. According to art. 62(6) LED and Recital 94 LED, the Commission should evaluate the compatibility between the LED and provisions of acts adopted prior to its adoption regulating the processing of personal data (such as Article 23 MLA Convention) in order to assess the need for alignment of those specific provisions with the LED; based thereon, the Commission is expected to make proposals with a view to ensuring consistent legal rules relating to the processing of personal data. Such exercise with regard to, among others, the EIO has been undertaken by the Commission in 2020. The sole introduced alignment was the deletion of Article 20 EIO and the inclusion of a reference to the applicability of the LED—without addressing whatsoever Article 23 MLA Convention.[56] Therefore, the Convention regime has not (as yet) been substituted by LED-based rules—even though, as the below analysis shows, Article 23 MLA Convention is incompatible with the LED as regards its three core strengths.

[56] European Commission (2020). Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar acquis with data protection rules (COM (2020) 262 final), p. 10.

A first incompatibility with the LED concerns the specialty-inspired allowance in Article 23.1, under (d), of further use based on consent of the data subject. As already pointed out above, such allowance in fact strengthens the procedural rights position of the person concerned, especially if the consent would be corroborated by additional guarantees, as in extradition or surrender contexts,[57] i.e. established in such a way as to show that the person concerned has consented expressly, voluntarily and in full awareness of the consequences, having had the right to legal counsel.[58] In addition, the possible non-consent of the person concerned should no longer be allowed to be circumvented by obtaining the consent of the requested state instead (*supra*).[59] This strength of the speciality rule seems to be in line with the 'unconventional' understanding of its function in the context of the EU law, in which, apart from preserving the sovereignty of the executing State, it also seeks to guarantee the rights of the person concerned.[60]

A second strength is that Article 23 MLA Convention frames a default use limitation to criminal justice purposes of information or evidence collected through MLA, i.e. 'for the purposes of proceedings to which [the] Convention applies', as scoped in its Articles 1[61] and 3.[62] It was already pointed out above that the value of such *meta* specialty principle is in its principled rejection of purpose deviation into the sphere of public or national[63] security. Whilst the EU MLA Convention only allows cross-over into the latter sphere when strictly necessary and proportionate, i.e. 'for the purpose of preventing an immediate and serious threat to public security' (Article 23.1, under (c)), the LED in fact fundamentally blurs the boundaries between criminal justice work and public security, by allowing ample

[57] Article 19 Benelux Extradition and MLA Treaty, Article 66 SIC, Article 7 EU Simplified Extradition Convention, Article 13 EAW.

[58] Whilst in extradition or surrender law this was typically ensured by requiring the person concerned to give consent before a judicial authority, in an MLA context, the assurances could be given in the form a written certification signed by the person concerned, attesting that he or she has had the right to be assisted by a lawyer before consenting, or directly by his or her counsel, as proposed in Article 19 of the draft Belgian code of international cooperation in criminal matters, drafted by Vermeulen et al., 2002, pp. 26, 134–135.

[59] '[…] the consent of the person concerned […] might indeed be a viable exception, but only if that consent – and with it, the purpose limitation principle – could not be circumvented when the member state consents instead' (Vermeulen & Ryckman, 2012, p. 100).

[60] Opinion of Advocate General Bobek in Case C-195/20 PPU, XC, ECLI:EU:C:2020:61, § 39.

[61] (a) The European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, hereinafter referred to as the 'European Mutual Assistance Convention'; (b) the Additional Protocol of 17 March 1978 to the European Mutual Assistance Convention; (c) the provisions on mutual assistance in criminal matters of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders which are not repealed pursuant to Article 2(2); (d) Chapter 2 of the Treaty on Extradition and Mutual Assistance in Criminal Matters between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands of 27 June 1962, as amended by the Protocol of 11 May 1974 (hereinafter referred to as the 'Benelux Treaty') in the context of relations between the Member States of the Benelux Economic Union.

[62] Proceedings brought by the administrative authorities in respect of acts which are punishable under the national law of the requesting or the requested member state, or both, by virtue of being infringements of the rules of law, and where the decision may give rise to proceedings before a court having jurisdiction in particular criminal matters, including those which relate to offences or infringements for which a legal person may be held liable in the requesting member state.

[63] The fact that, as laid down in recital 14, 'activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) [do not fall] within the scope' of the LED, does not prevent the police or other law enforcement authorities to collect dual-use information, i.e. for use in criminal and national security matters.

cross-over, under Article 4.2 LED,[64] to purposes relating to 'the safeguarding against and the prevention of threats to public security' (being purposes within the scope of the LED according to Article 1.1) whenever the additional purpose limitation test is passed, i.e. when authorised by Member State or Union law or necessary or proportionate to those purposes in accordance with Member State or Union law.

A third strength is the broadening foreseen in Article 23.1 (under (b)), i.e. for use in 'other judicial and administrative proceedings directly related to proceedings referred to under point (a)', which clearly goes beyond the subject matter of the LED. The procedures concerned, as explained in the Explanatory Report, cover inter alia: commercial proceedings related to following a fraudulent bankruptcy, proceedings for withdrawing parental authority related to criminal proceedings for the ill-treatment of children or proceedings for withdrawing a firearms licence related to criminal proceedings for violence with firearms. Chances that use in such proceedings meets the additional purpose limitation test of Article 4.2 LED seem low or inexistent, given that they surpass the narrow purposes of Article 2.1 j° 1.1 LED (i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'). Hence, if the LED philosophy would prevail in the future, it would essentially rule out the smart, functional and proportionate ('directly related') cross-over to other procedures, as currently allowed by Article 23.1, under (b) MLA Convention.

MLA would clearly be off worse when governed solely by the LED instead of by the MLA Convention regime. With the first two out of the above three strengths having their origin in the specialty principle, it moreover shows that MLA, as lacking genuine trust-building or trust-maintaining underpinnings, can hardly do without speciality, which prevents the bypassing of grounds or refusal or non-execution and enhances the rights of the person concerned (in particular in the EU MLA Convention fashion, i.e. by allowing the data subject a voice in the control process over the use of its data). In addition to punctual and context-specific speciality rules (as in the SIC for indirect tax matters; in Naples II for covert investigations; in the EU MLA Convention for spontaneous information exchange, newly obtained JIT-information and interception of communications; and in the EIO for interception of telecommunications), a fuller specialty rule would be beneficial, as a cornerstone for the trust required for free movement of information and evidence in the EU criminal justice area. The reality is that the EU persistently lacks trust-enhancing measures in the evidentiary field of cooperation and so grounds for non-recognition and non-execution remain legion also in a post-MR instrument like the EIO. The possibility of ex-post bypassing thereof in the absence of a generic specialty rule could well be detrimental for its future, especially since the EU has failed to implement Article 82.2 TFEU as concerns the possibility of adopting minimum rules in view of the mutual admissibility of evidence (European Commission, 2009; Vermeulen et al., 2010; Vermeulen, 2011a, 2011b; Raimundas and Zajančkauskienė, 2017; Kusak, 2019; Garamvölgyi et al., 2020). If investigative measures, like e.g. the interception of telecommunications, would have been (largely) harmonised as regards the offences for which they can be ordered (Kusak, 2016), there would have been no (or less) need for a provision as Article 11.1, under (h) EIO, which allows for non-recognition or non-execution where the use of an investigative measure ordered by an EIO is restricted under the law of the executing Member State to a list or category of offences or to offences punishable by a certain threshold which does not

[64] See also recital 29 LED.

include the offence covered by the EIO. In the absence of trust-enhancing measures, such as Article 82.2 TFEU-based commonly agreed EU (minimum) standards for investigative methods, only a generic specialty principle may really prevent the use of MLA-obtained information or evidence for other offences than granted for. Once evidence has gone abroad, the executing Member State currently has no control over it whatsoever. MLA, especially when involving intrusive measures, may also lead to severe harm to fundamental rights, as well confirmed by the European Court of Human Rights.[65] MR should not go as far as to prevent Member States to make sure that, where they have been requested or ordered to use intrusive techniques, the information or evidence thus gathered is not used abroad in connection with offences for which they consider such techniques disproportionate. The key question for the future is whether MR-based MLA, which can only thrive on an enhanced level of mutual trust, can do without a generic specialty or data ownership principle.

Funding The work of Martyna Kusak leading to this publication has received support from the National Science Centre, Poland, grant number 2015/19/B/HS5/00122.

Data Availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of Interest The authors declare no competing interests.

References

Bassiouni, M. (Ed.) (2008). *International Criminal Law.* Vol. 2: *Multilateral and Bilateral Enforcement Mechanisms.* Martinus Nijhoff.

Commissie tot bestudering van de positie van verdachten en andere belanghebbenden in de internationale strafrechtelijke samenwerking (1993). *Individu en internationale rechtshulp in strafzaken*, 's Gravenhage.

Conseil de l'Union européenne, 10198/95, *Note du Secrétariat Général du Conseil au Groupe "Entraide judiciaire en matière pénale": Questionnaire sur l'entraide judiciaire dans les matières pénales (Télex n° 3195 du 27 juillet 1995) – Réponses des* délégations, 21.

Conseil de l'Union européenne. (1995). 7193/95, Note de la Présidence en date du 16 mai 1995 au Groupe Directeur III: Séminaire d'entraide judiciaire organisé par la Présidence française à Bordeaux du 20 au 22 avril 1995. *JUSTPEN, 72*, 16.

[65] See, among others: *Allan v. United Kingdom,* App. no. 48539/99; *Big Brother Watch and Others. v. United Kingdom, Apps. nos. 58170/13, 62,322/14 and 24,960/15; Bykov v. Russia*, App. no. 4378/02; *Dragojević v. Croatia*, App. no. 68955/11; *Dumitru Popescu v. Romania,* App. (no. 2), no. 71525/01; *Gäfgen v. Germany,* App. no. 22978/05; *Kennedy v. United Kingdom*, App. no. 26839/05; *Khan v. United Kingdom,* App. no. 35394/97; *Klass and Others v. Germany,* App. no. 5029/71; *Kruslin v. France*, App. no. 11801/85; *Rotaru v. Romania,* App. no. 28341/95; *Schenk v. Switzerland,* App. no. 10862/84; *Zakharov v. Russia*, App. no. 47143/06.

Conseil de l'Union européenne, 8488/95, *Note de la future présidence espagnole au Groupe "Criminalité organisée internationale": Projet de questionnaire sur l'entraide judiciaire en matière pénale*, 26 June 1995.

Council of Europe. (2006). *Extradition European standards, Explanatory notes on the Council of Europe convention and protocols and minimum standards protecting persons subject to transnational criminal proceedings*. Council of Europe Publishing.

Council of the European Union (2016). Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area. 9368/1/16 REV1.

Csonka, P. (2006). The Council of Europe's Convention on Cyber-crime and other European initiatives. *Rev Int Droit Pénal, 3–4*(77), 473–501.

Drewer, D., & Ellermann, J. (2012). Europol's data protection framework as an asset in the fight against cybercrime. *ERA Forum, 13*, 381–395.

European Commission (2009). Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (COM(2009) 624 final).

European Commission (2020). Communication from the Commission to the European Parliament and the Council, Way forward on aligning the former third pillar acquis with data protection rules (COM(2020) 262 final).

Europol, Data Protection Office. (2011). *Data Protection at Europol.* Publications Office of the European Union. https://doi.org/10.2813/38585

Europol (2013). *EIS. Europol Information System. Crime reference system for EU law enforcement and cooperation partners.* Publications Office of the European Union, QL-32–13–058-EN-D.

Extract from the Conclusions of the 49th Plenary meeting of EJN. https://www.ejnforum.eu/cp/registry-files/3373/ST-15210-2017-INIT-EN-COR-1.pdf

Garamvölgyi, B., Ligeti, K., Ondrejová, A., & M. von Galen, M. (2020). Admissibility of Evidence in Criminal Proceedings in the EU. *Eucrim*, *3*, 201–208.

Kusak, M. (2016). *Mutual admissibility of evidence in criminal matters in the EU. A study of telephone tapping and house search*. Maklu.

Kusak, M. (2019). Mutual admissibility of evidence and the European investigation order: Aspirations lost in reality, ERA Forum. *Journal of the Academy of European Law, 19*(3), 391–401.

Lagodny, O., & Rosbaud, C. (2009). Speciality Rule. In N. Keijzer & E. Van Sliedregt (Eds.), *The European Arrest Warrant in Practice.* Springer.

Leiser, M. R., & Custers, B. H. M. (2019). The Law Enforcement Directive: Conceptual challenges of EU Directive 2016/680. *European Data Protection Law Review, 5*(3), 367–378.

Nagel, K.-F. (1988). *Beweisaufnahme im Ausland*. Max-Planck-Institut.

Orie, A. (1986). Internationale opsporing. In *Internationalisering van het strafrecht.* Ars Aequi Libri.

Orie, A., Van der Meijs, J., & Smit, A. (1991). *Internationaal strafrecht*. Tjeenk Willink.

Raimundas, J., & Zajančkauskienė, J. (2017). Movement of evidence in the European Union: Challenges for the European Investigation Order. *Baltic Journal of Law & Politics, 9*(2), 56–84.

Rozie, M. (Ed.). (1996). *Fiscaal Strafrecht en Strafprocesrecht.* Mys & Breesch.

Sajfert, J., & Quintel, T. (2020). Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. In M. Cole & F. Boehm (Eds.), *GDPR Commentary.* Edward Elgar Publishing.

Sjöcrona, J. (1990). De kleine rechtshulp. Nederlands procesrecht ten behoeve van buitenlandse justitie en politie. Een onderzoek naar de betekenis van de artikelen 552h-552q van het Wetboek van Strafvordering, Gouda Quint BV.

Stessens, G. (2000). *Money Laundering: A New International Law Enforcement Model*. Cambridge University Press.

Vavoula, N. (2017). EU immigration databases under scrutiny. Towards the normalisation of surveillance of movement in an era of 'Privacy Spring'? In G. Vermeulen, & E. Lievens (Eds.), *Data protection and privacy under pressure: transatlantic tensions, EU surveillance, and big data.* Maklu.

Vermeulen, G. (1999). *Wederzijdse rechtshulp in strafzaken in de Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de Lid-Staten?* Maklu.

Vermeulen, G. (2006). EU conventions enhancing and updating traditional mechanisms for judicial cooperation in criminal matters. *Revue Internationale De Droit Pénal, 77*, 59–95.

Vermeulen, G. (2011). *Free gathering and movement of evidence in criminal matters in the EU, Thinking beyond borders, striving for balance, in search of coherence*. Maklu.

Vermeulen, G. (2011b). Samenwerking met strafrechtelijke finaliteit in de EU. De autoriteitenstrijd voorbij, op zoek naar meer coherentie. In T. Spapens, M. Groenhuijsen, & T. Kooijmans (Eds.), *Universalis: Liber Amicorum Cyrille Fijnaut.* Intersentia.

Vermeulen, G. (2019). *Inclusion of data protection safeguards relating to law enforcement trans-border access to data in the Second Additional Protocol to the Budapest Convention on Cyber-crime (ETS 185), T-PD(2019) 3*. Council of Europe.

Vermeulen, G., De Bondt, W., & Van Damme, Y. (2010). *EU cross-border gathering and use of evidence in criminal matters. Towards mutual recognition of investigative measures and free movement of evidence?* Maklu.

Vermeulen, G., & Ryckman, C. (2012). Criminal justice finality: A decisive element in the development of international cooperation in criminal matters. In G. Vermeulen, W. De Bondt, & C. Ryckman (Eds.), *Rethinking International Cooperation in Criminal Matters in the EU: Moving Beyond Actors, Bringing Logic Back, Footed in Reality.* Maklu.

Vermeulen, G., Vander Beken, T., De Busser, E., Van den Wyngaert, C., Stessens, G., Masset, A., & Meunier, C. (2002). *Een nieuwe Belgische wetgeving inzake internationale rechtshulp in strafzaken*. Maklu.

Vogler, T. (1985). Spezialitätsbindung bei der sog. "kleinen" Rechtshilfe? *Goltdammer's Archiv für Strafrecht.* 195–202.

Zaïri, A. (1992). *Le principe de la spécialité de l'extradition au regard des droits de l'homme*. Librairie Générale de Droit et de Jurisprudence.

Legislation

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, European Treaty Series No. 181.

Convention drawn up on the basis of Article K.3 of the Treaty on European Union on mutual assistance and cooperation between customs administrations, OJ C 24, 23.01.1998.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108.

Convention of 10 March 1995, adopted on the basis of Article K.3 of the Treaty on European Union, drawing up the Convention on simplified extradition procedure between the Member States of the European Union, OJ C 78.

Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.09.2000.

Convention of 27 September 1996 drawn up on the basis of Article K.3 of the Treaty on European Union, relating to extradition between the Member States of the European Union, OJ L C 31, 23.10.1996.

Convention of 29 May 2000 established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.07.2000.

Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office, OJ C 316 of 27 November 1995.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office, OJ L 121 of 15 May 2009.

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, 30.12.2008.

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.07.2002.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, European Treaty Series No. 141.

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Council of Europe Treaty Series No. 198.

Council of Europe, Convention on Cybercrime, European Treaty Series No. 185.

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, OJ L 119, 4.05.2016.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.05.2014.
Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, OJ L 39, 21.02.2022, pp. 1–3.
European Convention of 13 December 1957 on Extradition, ETS No. 024.
European Convention of 20 April 1959 on Mutual Assistance in Criminal Matters, ETS No. 30.
European Convention of 28 May 1970 on the international validity of criminal judgments, ETS No. 070.
Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union, OJ L 327, 5.12.2008, as amended by Framework Decision 2009/299/JHA of 26 February 2009, OJ L 81, 27.03.2009.
Protocol of 22 November 2017 amending the Additional Protocol of 18 December 1997 to the European Convention on the transfer of sentenced persons, CETS No. 222.
Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135 of 11 May 2016.
Regulation (EU) 2019a/817 of the European Parliament and of the Council of 20 May 2019a on establishing a framework for interoperability between EU information sys-tems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135 of 22 May 2019a.
Regulation (EU) 2019b/818 of the European Parliament and of the Council of 20 May 2019b on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019b/816, OJ L 135 of 22 May 2019b.
Second Additional Protocol of 8 November 2001 to the European Convention on Mutual Assistance in Criminal Matters, European Treaty Series No. 182.
Traité du 27 juin 1962 d'extradition et d'entraide judiciaire en matière pénale entre le Royaume de Belgique, le Grand-Duché de Luxembourg et le Royaume des Pays-Bas, Mémorial (Journal Officiel du Grand-Duché de Luxembourg) A, No. 13, 22 March 1965.
Verdrag van 27 juni 1962 aangaande de uitlevering en de rechtshulp in strafzaken tussen het Koninkrijk België, het Groothertogdom Luxemburg en het Koninkrijk der Nederlanden, Tractatenblad van het Koninkrijk der Nederlanden, 1962, No. 97, Belgisch Staatsblad, 24 October 1967.

European Court of Human Rights Case Law

Allan v. United Kingdom. (2002). ECtHR, app. no. 48539/99.
Big Brother Watch and Othersv. United Kingdom. (2021). ECtHR, apps. nos. 58170/13, 62322/14 and 24960/15.
Bykov v. Russia. (2009). ECtHR, app. no. 4378/02.
Dragojević v. Croatia. (2015). ECtHR, app. no. 68955/11.
Dumitru Popescu v. Romania. (2007). ECtHR, app. (no. 2), no. 71525/01.
Gäfgen v. Germany, (2010). ECtHR, app. no. 22978/05.
Kennedy v. United Kingdom. (2010). ECtHR, app. no. 26839/05.
Khan v. United Kingdom. (2000). ECtHR, app. no. 35394/97.
Klass and Others v. Germany. (1978). ECtHR, app. no. 5029/71.
Kruslin v. France. (1990). ECtHR, app. no. 11801/85.
Rotaru v. Romania. (2000). ECtHR, app. no. 28341/95.
Schenk v. Switzerland. (1988). ECtHR, app. no. 10862/84.
Zakharov v. Russia. (2015). ECtHR, app. no. 47143/06.

The work described has not yet been published and is not under consideration for publication anywhere else. Its publication has been approved at the institutes where the work was carried out.